Bloomberg Law®

bloombergbna.com

Data Protection

INSIGHT: The GDPR's Reach on U.S. Non-Profits and Associations

By Elizabeth A. Rogers and Velvet D. Johnson, Michael Best & Friedrich LLP

May 25 marked the beginning of enforcement for the European Union's General Data Protection Regulation (''GDPR''), a sweeping revamp of prior EU privacy and cybersecurity laws. The regulation is aimed at enhancing the data privacy rights of individuals within the EU as it relates to the collection and processing of their personal data. The fortuitous timing of the enforcement date in the wake of a steady stream of news concerning privacy and cybersecurity revelations and data breaches seemed to serve as a prophetic response to these growing issues. Although the GDPR is an EU law, it has ripple effects around the world, including in the United States. Whereas U.S. privacy laws are mostly sectoral, the GDPR's industry-agnostic approach results in broad application, including to associations and non-profit organizations in the United States. Because of the large potential fines of 4% of worldwide revenue or up to €20 million, these entities need to be aware of whether the GDPR applies to them and, if so, what that means.

What kind of data does the GDPR regulate? The GDPR can apply to any type of organization or association, including non-profits. Its broad application depends on the activities of an organization rather than the industry or sector in which the organization operates. The regulation applies generally to ''the processing of personal data'' with a few exceptions. It is, therefore, critical to determine whether your non-profit or trade association processes personal data or sensitive personal data. If that is the case, then several obligations apply, including the need to establish a legal basis for processing the personal data under Article 6 and, if sensitive personal data is involved, the need to satisfy additional special conditions for processing under Article 9.

Under Article 4 of the GDPR, personal data broadly includes ''any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, culture or social identity of that natural person.'' GDPR, Art. 4(1). Accordingly, based on this broad description, it is clear that much of the data that associations and non-profits hold on their members, prospects, former members, sponsors, donors, meeting participants, etc. would be considered ''personal data.''

Sensitive personal data includes data that could create more significant risks to a person's fundamental rights and freedoms or puts them at risk of unlawful discrimination. It includes, for example, information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation. Processing of this data is prohibited without the explicit consent of the data subject or if one of the other conditions of Article 9 is satisfied.

Trade associations and non-profits must satisfy both Article 6 and Article 9 if they possess personal data and sensitive personal data. They do not have to be identical conditions. For example, if you rely on consent under Article 6 for processing personal data, you may rely on a basis other than consent to process sensitive personal data. Article 9(2)(d) provides a notable exception from the consent requirement in circumstances in which (1) the processing is performed in the course of an association or non-profit's normal business operations, (2) the data collected pertains to current and former members or persons with whom it has regular contact, and (3) the data is not released to third parties without the consent of the data subject.

How do I know if and how my association or non-profit is subject to the GDPR? There are three basic triggers for the GDPR: (1) physical presence in the EU, (2) offering goods or services to EU residents, and (3) tracking or monitoring of EU residents to serve targeted advertising or other marketing purposes. Any of the above is enough to trigger the GDPR. Even if you don't sell products to EU residents, for example, you still may be covered if you engage in ad-tracking of website visitors and don't exclude EU residents. So the GDPR would apply to an association located entirely within the United States if it offers its services—including providing informational services and member benefits, even if free—to those in the EU. It would also apply to a U.S. association if it monitors the behavior of those in the EU, for example through online tracking or retargeting of online ads.

What is the difference between a Data Controller and a Data Processor? A corollary question becomes whether your entity is a data controller or a data processor. The entity who determines the purposes and means of processing is the ''data controller.'' This is contrasted with a ''data processor,'' which processes personal data on behalf of the data controller. There are many changes for data processors under the GDPR, with many of the contractual obligations on them having been placed on a statutory footing. In practice, the distinction between a data controller and a data processor is often not easy to ascertain.

One way of looking at this is in the example of an association that outsources its IT services to a third party (think of an online database management application). This is not an unusual situation, especially for many associations that outsource the hosting of a website that may include an online membership directory, for example.

The association in this case would be considered the ''data controller'' because the association maintains ''control'' over the data (it is collected, maintained, and manipulated at the direction of the association). The third-party service provider would be considered a ''data processor'' because it has access to the data through the provision of its IT services.

What are my association's or non-profit's responsibilities? Associations and non-profits who have exposure under the GDPR should consider taking a number of steps immediately, even just as a matter of best practices:

- limit data usage to the purpose(s) for which data is originally collected;
- determine whether consent is required for marketing e-mails;
- adopt internal data security measures that conform to a standard suitable for your association's industry, e.g., NIST or ISO;
- inform EU residents about how their data will be used;
- be able to establish clear and unambiguous consent for use of data beyond the immediate purpose for which it was given or gathered;
- revise data processing agreements with third-party service providers (processors or sub-processors) and respond to individual requests of data subjects regarding the processing of their data;
- notify the competent data protection authority of data breaches;
- maintain a record of processing activities;
- delete personal data according to an established data retention policy; and
- under certain circumstances, designate a representative in the EU.

What are the penalties for non-compliance? Each supervisory authority has a range of investigative, corrective, executive, and advisory powers in order to ensure compliance with the GDPR, including the power to:

- issue warnings;
- order the data controller or the data processor to comply with a data subject's requests to exercise his or her rights under the GDPR;
- order the data controller to communicate a personal data breach to the data subject(s);
- impose a temporary or definitive limitation, including a ban on processing;
- order the correction or erasure of personal data or restriction of processing pursuant to a data subject's rights;
- impose an administrative fine; and
- order the suspension of data flows to a recipient in a third country or to an international organization.

In addition, fines that are quite staggering can be imposed on top of, or instead of, the corrective powers a supervisory authority has at its disposal:

- a fine of up to €10,000,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- a fine of up to €20,000,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year for the most severe forms of a breach and including violations of the basic principles of processing, including conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organization, or non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority.

Conclusion While some view May 25, 2018, as a deadline that has already passed, it is really just the beginning. GDPR enforcement has just started, and associations may be called upon to assist in reinforcing the data privacy rights of EU residents. GDPR Art. 80(1) permits organizations, associations, or non-profits that are active in the field of consumer data protection to file complaints with the appropriate supervisory authority and to represent aggrieved individuals in class action-like litigation. Associations should continue to evaluate

the applicability of the GDPR, understand their new authorities under the regulation, and take a systematic approach to compliance. Each association should understand the role it plays in the GDPR framework and how it processes EU data subjects' data in order to determine its obligations.

Author Information

Elizabeth A. Rogers (earogers@michaelbest.com) is a partner in the Austin office of Michael Best & Friedrich LLP. Velvet D. Johnson (vdjohnson@michaelbest.com) is senior counsel in the firm's Washington, D.C. office.

The views expressed in this article are those of the authors and not necessarily those of Michael Best & Friedrich or its clients, or of Bloomberg Law.