BDO USA

ARTICLE

April 10, 2024

BY:

Karen Schuler

Principal; Head of Global Privacy & Data Protection

Empowering Users: Unleashing the Data Rights Revolution

Since the introduction of the European Union's (EU) General Data Protection Regulation (GDPR) in 2018, the privacy rights afforded to individuals have rapidly expanded across the world in general and in the United States in particular. There have been 13 state privacy laws signed since the GDPR took effect and this number is rapidly increasing as more states recognize individuals' right to exercise greater control over their personal information. While nonprofit organizations (NPOs) are largely exempt from many of the obligations imposed domestically, there are several steps that should be taken to address international responsibilities and the continually changing privacy landscape.

U.S. State Privacy Landscape

In addition to the list of U.S. legislation depicted below, there are more than 25 data privacy or protection bills in committee across 11 states at press time. This momentum will continue to push the introduction and implementation of privacy laws across the U.S. While these laws are not explicitly regulating the processing of personal data, there are generally recognized responsibilities concerning donor information that NPOs should address. This ambiguity can confuse the appropriate categorization of an NPO. The California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA) for example, contains an additional definition of “business” that may impact NPOs that share common branding with a for-profit business or are controlled by a business through director elections, management decisions or voting power. These factors can pose significant risk to NPOs' compliance requirements.

State	Signed	Effective
California	2018 (Amended 2020)	Jan. 1, 2020 (Amended 2023)
Colorado	2021	July 1, 2023
Connecticut	2022	July 1, 2023
Delaware	2023	Jan. 1, 2025
Indiana	2023	Jan. 1, 2026
Iowa	2023	Jan. 1, 2025
Montana	2023	Oct. 1, 2024
New Jersey	2024	Jan. 15, 2025
Oregon	2023	July 1, 2024
Tennessee	2023	July 1, 2025
Texas	2023	July 1, 2024
Utah	2022	Dec. 21, 2023
Virginia	2021	Jan. 1, 2023

*Current as of Jan. 31, 2024

While the individual rights afforded to residents differ by state, the following rights are generally included:

- Right of access by the data subject
- Right to correction
- Right to delete
- Right to opt out of certain processing/sales
- Right to data portability
- Right to opt in for sensitive data processing
- Right to not be subject to automated decision-making

These rights are not only dependent on the state where a data subject resides, but also the sensitivity of the data involved in the processing.

Global Privacy Landscape

Unlike U.S. state privacy laws, global privacy laws apply to entities that process the personal data of their residents. The EU GDPR, for example, defines applicable entities as either “Controllers” or “Processors.” Controllers are individuals or entities that determine the purposes and means of processing, whereas Processors are individuals or entities that process personal data on behalf of the Controller. NPOs should be aware of the following conditions that would make the EU GDPR applicable to their organization:

- Processing of personal data by an organization established in the EU.
- Processing of personal data of data subjects by an organization not in the EU where processing is related to:
  - Offering goods or services, irrespective of payment of the data subject, to data subjects in the union; or
  - Monitoring of their behavior when that behavior takes place within the EU.

- If processing takes place where EU Member State law applies by virtue of public international law. (e.g., Member State embassies and consulates, Member State cruise ships traveling in international waters)

Once an NPO is considered a Controller under the GDPR, there are certain obligations that must be met to become compliant and avoid fines by the supervisory authorities of EU countries. One critical obligation is the fulfillment of data subject rights. The fulfillment of these rights begins with the transparent communication of them to the data subject. A response must also be provided to the data subject within a calendar month (30 days). These rights include the following:

- Right of access by the data subject
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object to processing
- Right to not be subject to automated decision-making

These rights can pose a serious challenge to NPOs. One of the most efficient methods of addressing this challenge is through the development and implementation of policies and procedures to efficiently address these obligations. These policies and procedures manage the end-to-end fulfillment of the data subject rights requests from intake and ID verification to the appropriate response and completion of the request. By operationalizing the process of fulfilling any rights requests received, NPOs can reduce the risk of noncompliance which can carry significant financial penalties.

Have Questions?
Contact Us.

Return to Nonprofit Standard Newsletter