State Data Privacy Brief

Contents

- Key findings
- Contents
- Why a nonprofit can't assume it's exempt
- Sorting which states' laws actually apply
- What member and donor data typically falls inside the laws' scope
- Remote staff and out-of-state obligations
- Breach notification across a multistate footprint
- Building a practical review checklist

Key findings

- Several state consumer privacy laws exempt nonprofit organizations outright; others exempt them only partially, or not at all, and an association cannot assume the exemption that applies in its headquarters state applies everywhere its members and staff sit.
- Remote staff working from a state different from an association's headquarters can independently trigger that state's privacy obligations, regardless of where the association itself is incorporated or based.
- Breach-notification requirements differ enough by state that a single incident touching member data in several states can require several different notification timelines and content requirements running at once.
- Member and donor data most likely to draw scrutiny is the data that identifies an individual member as belonging to an underlying category the association serves, not just contact and billing information.

Contents

- Why a nonprofit can't assume it's exempt
- Sorting which states' laws actually apply
- What member and donor data typically falls inside the laws' scope
- Remote staff and out-of-state obligations
- Breach notification across a multistate footprint
- Building a practical review checklist

Why a nonprofit can't assume it's exempt

State consumer privacy laws were largely written with commercial data brokers and large consumer-facing businesses in mind, and several of them exempt nonprofit organizations from coverage entirely. That fact leads a lot of association staff to assume their own organization is categorically exempt from every state's law, which is not a safe assumption. Some states extend a nonprofit exemption only to certain categories of data or certain kinds of processing, and a handful apply their consumer privacy law to nonprofits without any special exemption at all. An association with member organizations, donors, and staff spread across several states is, in practice, operating under several different answers to the same exemption question simultaneously.

Sorting which states' laws actually apply

The starting point for any association's privacy review is not "does our state exempt nonprofits" but "which states' laws could reach us at all, and does each one exempt us." A state's consumer privacy law can apply to an organization based on where its consumers or members reside, where its staff sit, or in some cases where it's incorporated, and the specific trigger differs by statute. An association headquartered in one state, with chapter staff working from several others and members in all fifty, needs to work through each relevant state's applicability threshold and nonprofit exemption separately rather than relying on a single answer that covers the whole footprint.

What member and donor data typically falls inside the laws' scope

Basic contact information — name, mailing address, email — is the least likely category to draw scrutiny on its own, since it resembles ordinary business correspondence data most laws don't focus on closely. The more sensitive category, and the one associations should review most carefully, is data that reveals something about an individual beyond simple contact information: health-related membership categories (a nurses' association's membership list, for example, implicitly identifies licensed health professionals), financial data tied to dues or donation history, or any data an association collects specifically because of the professional or personal category its membership serves. The more a membership record says about who a person is, rather than just how to reach them, the more carefully it should be reviewed against each applicable state's definition of covered personal data.

Remote staff and out-of-state obligations

A pattern that catches many associations off guard is the effect of their own remote or hybrid staffing on privacy-law applicability. An association headquartered in a state with a nonprofit exemption can still find itself subject to another state's privacy law simply because it employs remote staff who reside and work in that other state, if that state's law is triggered by where data processing activity occurs rather than only by where the organization itself is based. As more associations hire remote staff outside their headquarters state, this trigger has become more relevant than it was when most association staff worked from a single office.

Breach notification across a multistate footprint

Breach-notification laws are older and more widespread than the newer consumer privacy statutes, and nearly every state has its own version, each specifying its own timeline for notifying affected individuals, its own definition of what counts as a reportable breach, and in some cases its own requirement to notify a state attorney general or consumer protection office. An association whose membership spans many states can find a single data incident — a stolen laptop, a compromised email account, a vendor breach affecting member records — triggering several different states' notification clocks simultaneously, each with a different deadline and a different required notice format. Building a breach-response plan around a single generic notification letter, rather than a state-by-state checklist prepared in advance, is one of the more common gaps this brief identifies in association data-handling practices.

Building a practical review checklist

Kavanagh-Pratt recommends associations build their own review around four questions, worked through methodically rather than answered all at once from memory: Which states does our membership, donor base, and staff footprint actually touch? For each of those states, does its privacy law exempt nonprofits, and if so, does the exemption cover all of our data or only some of it? Which of our own data categories look more like sensitive personal data than ordinary

contact information, under each applicable state's definition? And do we have a breach-notification plan that accounts for more than one state's timeline running at once?

Answering these questions once, in writing, and revisiting the answer whenever the association's staff footprint or membership base changes meaningfully, is a more durable approach than relying on a general sense that "we're a nonprofit, so this doesn't apply to us" — an assumption this brief's review of current state law does not support as a blanket rule.