I Can't Even.

The Overwhelmed Nonprofit's Guide to Data Privacy

Written by: Brian T. Sniffen

Nonprofits are generally subject to data-privacy laws. And compliance with those laws is key to avoiding data breaches, lawsuits, and fines. It's also important to establishing and maintaining the trust of donors, employees, and other constituents.

But determining what laws apply, and figuring out how to comply, is daunting. For example, Oregon nonprofits are likely subject to the Oregon Consumer Identity Theft Protection Act because they likely receive the personal data of Oregon residents—such as donors and employees. *See* ORS 646A.600 et seq. But that is probably just the tip of the iceberg: if the nonprofit also processes the personal data of people from other states, it is likely subject to those other states' data-privacy laws as well. Thus, a nonprofit that has donors from 35 different states is likely subject to the data-privacy laws of each of those 35 states. If donors are in the European Union, the EU's far-reaching General Data Protection Regulation ("GDPR") probably applies. It goes on and on.

So where do you start? Baby steps. Recognizing that action is better than inaction, this article summarizes, in four steps, how to start working toward compliance. If you follow these steps, you'll be amazed at the progress you make.

1. Determine What Personal Data Your Nonprofit Processes, and What It Does With That Data.

The first question to ask is "What personal data does my nonprofit process?" "Personal data" includes name, address, e-mail address, phone number, Social Security number, driver's license number, health information, financial information, and any other sensitive information that could be used to identify someone or commit identity theft. "Process" means "collect, access, store, transmit, use, share, or sell."

The second question to ask is "Where do these people live?"

The third question to ask is "What does my nonprofit do with the personal data?" Is it shared with third parties (e.g., with other nonprofits for mailing lists or promotional activities)? Is it sold?

The answers to the first two questions are important as you start to identify applicable law (see Step #2, below). For many nonprofits, credit card and personal contact information for donors is collected. Any nonprofit with employees also processes the personal data of those employees. The third question is important to start thinking about whether your disclosures regarding these practices are accurate, and whether your practices might run afoul of applicable law.

2. Determine What Laws Apply.

The United States has no omnibus nationwide data-privacy law: each state has its own law. At the federal level, the data-privacy laws are generally organized around the type of data involved. Cataloguing all the potential laws that could apply is not possible in this article. But here are some of the laws that frequently apply to nonprofits:

- *State law*. The state law that applies is determined by the data subject's residency. So if your nonprofit has employees or donors in California, Oregon, and Washington, those states' laws will apply. Review them to see what they require. Differences in state laws include different definitions of "personal data," security requirements, deadlines and required content for data-breach notifications, and enforcement mechanisms. State attorneys general also have the ability to take action against unlawful trade practices—such as improper or misleading uses of personal data.
- *Federal law*. At the federal level, the Federal Trade Commission has broad discretion to take action against unfair or deceptive trade practices—often manifesting that power through enforcement actions against companies whose website privacy policies make inaccurate statements about data collecting and sharing practices. The following list reflects some other federal laws that frequently arise with nonprofits:
    - The Children's Online Privacy Protection Act generally prohibits the collection of data from children under 13 without verifiable parental consent.
    - The Family Educational Rights and Privacy Act protects education records.
    - The Gramm-Leach-Bliley Act requires financial institutions (broadly defined) to protect private information and make certain disclosures.

    - The Health Insurance Portability and Accountability Act requires covered entities to protect health information.
    - The Telephone Consumer Protection Act generally prohibits autodialer calls and text messages to cell phones without consent.
- *International law*. If your nonprofit processes a foreigner's personal data, the laws of that person's home country may apply—even if the nonprofit has no physical presence in that country. A recent example of this extraterritorial application is the GDPR, which applies to companies of all sizes that process the personal data of people located in the EU—regardless of where the companies are located.
- *Other*. Not all data-privacy requirements are government-mandated laws. Some requirements are pushed through by contract. For example, if you process credit card transactions from a brand such as Visa, MasterCard, American Express, or Discover, you are committing to comply with the Payment Card Industry Data Security Standard—an extensive set of rules for securely processing those transactions—and are subject to fines if you do not. Similarly, key funding sources or other constituents may require you to uphold certain security standards.

3. Take Steps to Comply.

Once you know what personal data you process, how you process it, and what laws may apply, dig into those laws' requirements and prohibitions. You may discover that you are using or sharing data in an authorized way. You may also discover that your disclosures related to personal data are inaccurate. In either case, you can now take steps to improve your practices.

If you're looking for some common compliance themes for all these U.S. federal and state laws, here's a nonexclusive list:

- Do your best and learn from your mistakes. Regulators (and courts) don't require perfection, but they do require reasonable good-faith efforts at compliance, and action to address known vulnerabilities. What's "reasonable" depends on the organization's size and complexity, and the sensitivity of the personal data at issue.
- Relatedly, use reasonable administrative, technical, and physical safeguards to protect personal data. See ORS 646A.622 for the safeguards required for many Oregon companies. Reasonable safeguards might include:

    - Designating someone to take the lead on developing and implementing a security program, and on regularly deploying software updates and patches.
    - Identifying and evaluating risks regularly and in light of existing safeguards.
    - Training employees and working to establish a culture of security awareness.
    - Limiting access to data. Only those people who need personal data to perform their jobs should have access to it. Use multifactor authentication to reduce the risk of unauthorized access to electronic data and fraudulent wire transfers. Lock doors to restrict access to personal data in paper form.
    - Using and monitoring technical security measures, such as antivirus software, spam and malware filters, firewalls, and encryption. Encrypt personal data at rest and in transit. Encrypt personal data on removable media. Evaluate and update these measures as technology and risks evolve.
    - Ceasing the collection of data you don't need. Securely destroy what you can. Identify your record-retention requirements and then set up a destruction schedule.
- Be accurate and transparent about your data collection and use practices. Look at your website privacy policy and revise it to reflect reality.
- Negotiate your vendor contracts to match your obligations/level of data sensitivity (or get new vendors). If possible, insist on the following provisions:
    - You should own your data, and the vendor should only be able to use it to provide you with the services you requested.
    - The vendor's data-security obligations should match the security requirements mandated by law for the data being processed.
    - The vendor should indemnify you if it fails to live up to its promises.
    - The vendor should be required to provide you with timely notification if it suffers a data-security incident involving your data.
    - The vendor's damages cap should be meaningful in light of the risk involved.
    - Insurance coverage, including cyber insurance. While cyber policies are far from uniform, insurance coverage should at least be considered. (Aside from contract negotiations, consider whether your nonprofit would benefit from cyber insurance coverage.)

4. Draft an Incident-Response Plan; Practice, Practice, Practice.

Finally, even after making huge improvements in your privacy program, data-security incidents still might happen. So have a plan in place—particularly because incident-response plans greatly reduce the overall costs of data-security incidents. And anecdotally, "winging it" adds a lot of stress to an already stressful situation.

What does a good incident-response plan include? It depends on the organization, but when putting one together you should consider these questions:

- How should employees escalate incidents to the incident-response team?
- Who's on the incident-response team, and what is each person's responsibility? Attorneys (think attorney-client privilege and work-product protection), bankers, forensic experts, insurers, law enforcement, members of your executive team, members of your PR team, and members of your IT team may all have a role. List these people and their contact information.
- What are the protocols for issuing press releases and other communications related to the incident?
- Whom must you notify? What personal data, if compromised, triggers a formal reporting obligation? Which state and federal regulators, if any, must be notified? What contracts require you to notify the other party? What are the deadlines for reporting?

Your nonprofit should run through mock exercises to identify gaps or practical problems with your incident-response plan. And the plan should be regularly adjusted to reflect current personnel and practices. Finally, keep a hard copy of your plan handy in case your computer network is unavailable or otherwise compromised.

As the ancient Chinese proverb states, "A journey of a thousand miles begins with a single step." I hope this article helps you take those first steps toward compliance.

Brian is a partner at the law firm of Miller Nash Graham & Dunn, providing outside general counsel services to clients that need cost-effective advice on all manner of contracts and corporate governance. He also provides advice to companies that need assistance on certain specialty subjects, such as data privacy and data security, or that need extra bandwidth for negotiating complex agreements. Brian can be reached by phone at 503.205.2443 or by email at brian.sniffen@millernash.com