PRO BONO BRIEF™
NONPROFIT LEGAL NEWS
February 9, 2022

This article presents general guidelines for Ohio nonprofit organizations as of the date written and should not be construed as legal advice. Always consult an attorney to address your particular situation.

Ohio's Proposed Privacy Law and Your Privacy Program

Bruce F. Martino, CIPP/G, CIPM, *Whiteford, Taylor & Preston, LLP*

Ohio House Bill No. 376, the Ohio Personal Privacy Act (OPPA), was introduced in the Ohio legislature in July 2021. OPPA continues a trend of laws passed in the European Union, California, Colorado and Virginia, and being considered in states such as Washington and Oklahoma. These laws are aimed at giving consumers more control over the way businesses use their personal information (PI). It is important to remember that the OPPA is just a proposed law at this time. It will be debated in the Ohio legislature in the coming months. The bill, if passed, may differ from the version of the OPPA which was introduced.

A. OPPA Summary

OPPA is based on two core concepts – transparency and choice. OPPA requires businesses to tell consumers how the business will use the consumer's PI. Businesses typically use a website privacy policy to convey this information.

OPPA gives consumers a right of choice. Consumers have a right to request that a business provide the consumer with a copy of the PI the business maintains on the consumer. A consumer has the right to ask a business to delete the PI the business maintains on that consumer. Every consumer has the right to advise a business to not sell his or her PI to third parties.

Business is defined as any corporation, limited liability corporation or other group. It includes for profit and nonprofit entities. It does not include public entities such as cities, townships and counties. It is important to remember that not every business must comply with the OPPA. A business must meet one of the thresholds mentioned in the law for OPPA to apply. The business must either:

- Generate $25,000,000.00 in gross annual revenue in Ohio; or,
- Control or process the PI of at least 100,000 consumers; or,
- Generate at least 50% of its gross revenue from the sale of PI, and control or process the PI of at least 25,000 consumers.

Any nonprofit that meets one or more of the three criteria should a consult a privacy attorney.

B. Your Privacy Program

Even if the OPPA does not apply to your nonprofit, it is important to implement a risk-based privacy program. Nonprofits can hold PI that is valuable to bad actors. All organizations store and process PI about their employees, and many nonprofits store and process PI about their donors, clients, and volunteers.

PRO BONO PARTNERSHIP OF Ohio

There are six steps a business should take to implement a privacy program. They are:

1. **Data Mapping/Data Classification.** Many businesses do not know the systems and databases in which the PI they collect is processed and stored. In addition, many businesses use third parties to process and store PI. Data mapping is a process by which a business locates its PI and tracks it to each system used to process and store the PI. Do not forget PI stored in hard copy.

   PI should be classified after it is located. PI usually falls into one of three categories: public information; proprietary but not PI; and PI.

2. **Risk Assessment.** A business should then assess the risk around processing and storing its PI. Measure current practices against a set of industry standard data handling practices. Remediate the gaps.

3. **Policy, Process, and Procedures.** Written privacy and security policies, processes, and procedures related to handling and storing information should be adopted. Regulators will ask for these if the business is investigated.

4. **Incident Response Plan (IRP).** Every organization needs an IRP. The IRP sets out procedures that will be followed when the business has a known or suspected security incident or data breach.

5. **Training.** Many security incidents occur because well-meaning people are not careful or knowledgeable. Training staff and volunteers on secure data handling practices is crucial. For example, train staff on what to look for in spotting a phishing email. Studies show that staff members who have been trained are far less likely to open a phishing email.

6. **Audit.** Audit your privacy program and remediate gaps. Strive for constant improvement.

Finally, Ohio has had a breach notification law in effect since 2007. A business that suffers a breach of PI must notify the affected individuals of the breach. Nonprofit organizations are not excluded even in cases where the OPPA does not apply. Breaches can be costly and cause reputational damage. Building an effective privacy program and using reasonable security measures lessens the chance of a data breach.

Need Legal Advice?

If you are a PBPO client and have questions regarding the content of this article or need legal assistance, please contact us at info@pbpohio.org or (513) 977-0304.

Not a Client? Apply to become a client by submitting a Request for Legal Assistance online, or contact us at info@pbpohio.org.

About the Author:

Bruce Martino is Director of Privacy, Data Security & Compliance for Whiteford, Taylor & Preston, LLP. He is responsible for mitigating risk by creating sustainable legal strategies to ensure data privacy and security across all markets.

PRO BONO PARTNERSHIP OF Ohio