INTERNATIONAL LAWYERS NETWORK

2024 ILN DATA PRIVACY GUIDE

An International Guide

www.iln.com

ILN Cybersecurity & Data Privacy Group and ILN Technology Media & Telecommunications Group

Disclaimer

This guide offers an overview of legal aspects of data protection in the requisite jurisdictions. It is meant as an introduction to these marketplaces and does not offer specific legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship, or its equivalent in the requisite jurisdiction.

Neither the International Lawyers Network or its employees, nor any of the contributing law firms or their partners or employees accepts any liability for anything contained in this guide or to any reader who relies on its content. Before concrete actions or decisions are taken, the reader should seek specific legal advice. The contributing member firms of the International Lawyers Network can advise in relation to questions regarding this guide in their respective jurisdictions and look forward to assisting. Please do not, however, share any confidential information with a member firm without first contacting that firm.

This guide describes the law in force in the requisite jurisdictions at the dates of preparation. This may have been some time ago and the reader should bear in mind that statutes, regulations, and rules are subject to change. No duty to update information is assumed by the ILN, its member firms, or the authors of this guide.

The information in this guide may be considered legal advertising.

About the ILN

The ILN is a non-exclusive network of high-quality mid-sized law firms, which operates to create a global platform for the provision of legal services, particularly for clients with international needs. With a presence in 67 countries, it is exceptionally well placed to offer seamless legal services, often of a cross-border nature from like-minded and quality legal practices. In 2021, the ILN was honored as Global Law Firm Network of the Year by The Lawyer European Awards, and in 2016, 2017, 2022, and 2023 they were shortlisted as Global Law Firm Network of the Year. Since 2011, the Network has been listed as a Chambers & Partners Leading Law Firm Network, increasing this ranking in 2021 to be included in the top two percent of law firm networks globally. Today, the ILN remains at the very forefront of legal networks in its reach, capability, and depth of expertise.

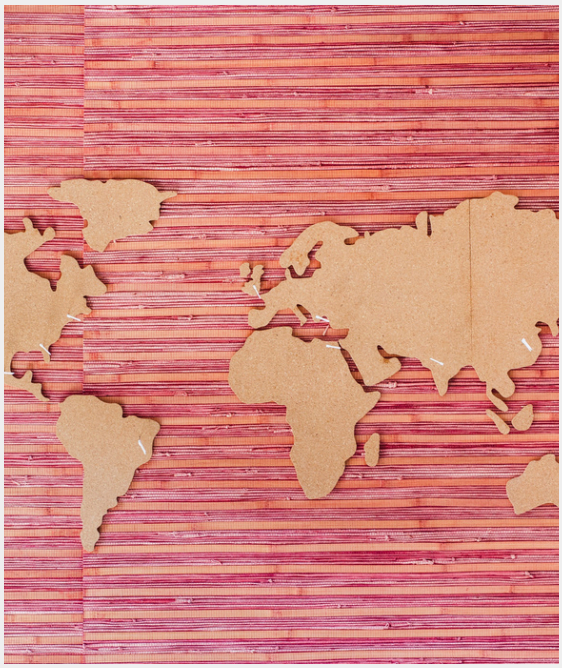
Authors of this guide:

1. Cybersecurity & Data Privacy Group

Co-chaired by Jim Giszczak of McDonald Hopkins and Stuart Gerson of Epstein Becker & Green, the Cybersecurity & Data Privacy Specialty Group provides an international platform for enhanced communication, enabling all of its members to easily service the needs of their clients requiring advice.

2. Technology, Media & Telecom (TMT)

Co-chaired by Alishan Naqvee of LexCounsel in New Delhi and Gaurav Bhalla of Ahlawat & Associates in New Delhi the TMT Group provides a platform for communication on current legal issues, best practices, and trends in technology, media & telecom.



www.iln.com

USA – Ohio

McDonald Hopkins' national data privacy and cybersecurity attorneys have a wealth of experience advising clients in a myriad of industries on the rapidly changing state, federal, international, and industry privacy and breach notification laws. McDonald Hopkins provides support on a daily basis and during investigations by state and federal regulators, as well assistance with:

- *Breach coaching and incident notification*
- *International privacy compliance*
- *Payment cards and ecommerce*
- *Privacy litigation and class action*
- *Proactive measures and breach compliance*
- *Regulatory investigation and government response*
- *Vendor relationships*

Introduction

In recent years, Ohio has made unique and nationally-mirrored efforts toward advancing a goal of protecting the personal data of its residents. In addition to joining other U.S. states in 2005 by requiring companies to notify consumers of breaches of their personal data,[1] Ohio was the first state in the nation in 2018 to enact legislation – the Ohio Data Protection Act ("DPA") - providing businesses a specific legal incentive to maintain cybersecurity programs for the protection of personal data. A limited number of other jurisdictions, such as Utah, have since taken similar incentive-based approaches to rewarding businesses that take specified action toward enhancing their cybersecurity postures and the protection of personal data.

Additionally, in 2021 Ohio joined the ranks of an expanding set of states across the U.S. that have introduced comprehensive consumer data privacy legislation that, if enacted, would fundamentally change the existing privacy landscape by providing Ohioans with newfound rights pertaining to their personal data. If enacted, OPPA would also impose new requirements on covered businesses to comply with specific privacy and cybersecurity-related requirements such as the posting of a privacy policy and maintenance of physical, technical, and administrative safeguards to protect the security of the personal data.

[1] See Ohio Rev. Code 1349.19

Contact Us

+1 (216) 348-5400
https://www.mcdonaldhopkins.com/
jgiszczak@mcdonaldhopkins.com
600 Superior Avenue E., Suite 2100
Cleveland, Ohio 44114-2653 USA

This article explores the core components of both OPPA and the Ohio DPA, assesses the new requirements for Ohio businesses under this emerging framework, and forecasts the new rights Ohioans may soon enjoy pertaining to the protection of their personal information.

Governing Data Protection Legislation

2.1.Ohio Data Protection Act (DPA) – Existing

In 2018 Ohio took the trailblazing step of enacting the Ohio Data Protection Act (DPA), which provides companies that implement specified cybersecurity programs a legal "safe harbor" in actions against them pertaining to data breaches.

Specifically, the Ohio DPA was the first such law in the nation to offer covered entities who implement specified cybersecurity programs an affirmative defense to specific causes of action sounding in tort.[1] Applicable causes of action must be brought under Ohio law or in Ohio court. Additionally, for the affirmative defense to apply, the cause of action must allege "that failure to implement reasonable information security controls resulted in a data breach concerning personal or restricted information."[2]

Given the ever-increasing cadence of data privacy-related litigation stemming from consumer-plaintiffs whose personal information is involved in data breaches, the Ohio DPA incentivizes Ohio businesses to take steps to protect personal information that they may otherwise not take. Although narrow in scope in that it may apply only after specified allegations are made, the Ohio DPA is unique in that it takes an incentive-based (as opposed to punitive-based) approach to achieve a desired outcome whereby the overall security of consumer data is enhanced through efforts made by companies that process such data to create cybersecurity programs.

2.2.Ohio Personal Privacy Act (OPPA) – Introduced

In addition to its novel enactment of the DPA, Ohio is also following in the footsteps of an expanding set of U.S. states – such as California, Connecticut, Colorado, Utah and others - that have enacted comprehensive consumer data privacy legislation. Specifically, in 2021 Ohio introduced House Bill 376, known as the Ohio Personal Privacy Act ("OPPA"), to the Ohio House of Representatives. If ultimately enacted, OPPA would provide consumers with enumerated and hallmark rights pertaining to the use and maintenance of their personal data that are mirrored in the comprehensive data privacy legislation elsewhere in the country. In addition to affording consumers with specific rights pertaining to the processing of their personal data, OPPA would also require businesses

[1] Ohio Rev. Code, 1354.02(D)
[2] Id.

to maintain safeguards and offer consumers a specified level of transparency with respect to their procedures pertaining to the collection and use of personal data through the conspicuous posting of a privacy policy.

Scope of Application

The Ohio DPA and proposed OPPA both specify the nature of the information that is being protected by the respective legal framework. Only specific information, such as "personal information" as defined under Ohio's DPA or "personal data" as defined under OPPA, rise to the level of triggering certain rights and obligations as applicable.

Additionally, if enacted, OPPA would mirror existing and proposed comprehensive consumer data privacy legislation in limiting its application to certain businesses based on factors such as (1) the connection that the business has to Ohio through physical presence and/or targeting of Ohio consumers, (2) the annual gross revenue of the business, (3) the volume of personal data processed by the business, and (4) amount of revenue the business derives from the sale of personal data.

3.1. Definition of Personal Information and Restricted Information (Ohio DPA)

The incentive-based Ohio DPA incorporates the definition of "personal information" from Ohio's previously-enacted data breach notification statue (Ohio Rev. Code, 1349.19), which defines "personal information" as:

[A]n individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable:

- Social security number;
- Driver's license number or state identification card number; or
- Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.[1]

Under the Ohio DPA, "Personal information" does not include "publicly available information that is lawfully made available to the general public from federal, state, or local government records and certain widely-distributed media."[2]

The Ohio DPA also defines "restricted information" as "any information about an individual, other than personal information, that, alone or in combination with other information, including personal information, can be used to distinguish or trace the individual's identity or that is linked or linkable to

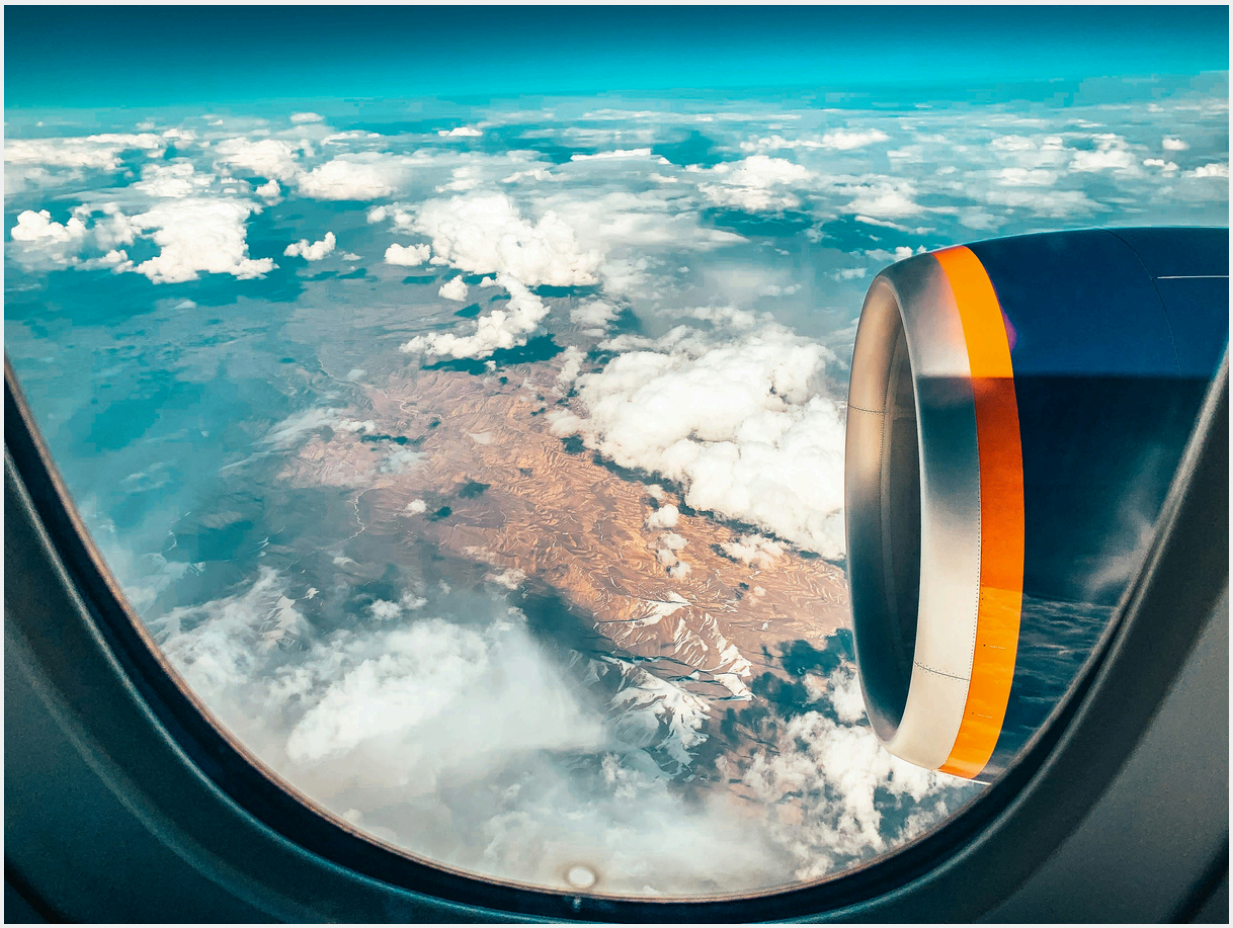
[1] Ohio Rev. Code, 1347.12(A)(7)(a)
[2] Id.

an individual, if the information is not encrypted, redacted, or altered by any method or technology in such a manner that the information is unreadable, and the breach of which is likely to result in a material risk of identity theft or other fraud to person or property."[1]

The concepts of both "personal information" and "restricted information' are integral to the foundation of the DPA in that, for a business to enjoy an affirmative defense under the DPA, the legal cause of action brought against the business seeking to employ the affirmative defense must allege a failure to implement reasonable information security controls resulted in a data breach concerning personal or restricted information.[2] Moreover, personal information is foundational to the affirmative defense in that the cybersecurity

[1] Ohio Rev. Code, 1354.01(E)

[2] Ohio Rev. Code, 1354.02(D)



program that is maintained must contains administrative, technical, and physical safeguards for the protection of personal information.[1]

3.2. Definition of Personal Data (OPPA)

If enacted in its current version, OPPA would mirror existing and proposed comprehensive consumer data privacy legislation elsewhere throughout the U.S. in defining "personal data" broadly as "any information that is linked or reasonably linkable to an identified or identifiable consumer and that is processed by a business for a commercial purpose."[2] Personal data would not include "data processed from publicly available sources" or "Pseudonymized, deidentified, or aggregate data."[3]

Statutory Exemptions

If enacted in its current version, OPPA would exempt certain personal data regulated by the Children's Online Privacy Protection Act (COPPA), and protected health information under the Health Insurance Portability and Accountability Act (HIPAA).[4] Additionally, OPPA would not apply to Ohio state agencies, financial institutions governed by the Gramm-Leach-Bliley Act (GLBA), and institutions of higher education. Business to business transactions would also be exempt under OPPA. [5]

[1] Ohio Rev. Code, 1354.02(A)(1)
[2] Ohio Personal Privacy Act, Sub. H. B. No. 376, 134th General Assembly
[3] Id.
[4] Id.
[5] Id.

3.3. Covered Entities – Ohio's DPA

Under the DPA, Ohio extends the benefit of an affirmative defense to "covered entities," which are defined broadly as "a business that accesses, maintains, communicates, or processes personal information or restricted information in or through one or more systems, networks, or services located in or outside this state (Ohio)."[5]

3.4. Covered Entities - OPPA

If enacted in its current version, OPPA would apply much more narrowly than the DPA only to businesses that either conduct business in Ohio or "produce products or services targeted to consumers in" Ohio)," and that satisfy one or more of the following:

·The business's annual gross revenues generated in Ohio exceed twenty-five million dollars;
·During a calendar year, the business controls or processes personal data of one hundred thousand or more consumers; or
·During a calendar year, the business derives over fifty per cent of its gross revenue from the sale of personal data and processes or controls personal data of twenty-five thousand or more consumers.[6]

[5] Ohio Rev. Code, 1354.01(B)
[6] Ohio Personal Privacy Act, Sub. H. B. No. 376, 134th General Assembly

Key Stakeholders

OPPA specifies key stakeholders whose rights and/or obligations are impacted by the respective legislation. OPPA mirrors comprehensive data privacy legislation at the national level in setting forth specific definitions of "business," "processors," and "consumers." The category that a person or entities falls into would ordinarily depend on their relationship and connection to personal data.

Business

Under OPPA "Business" would be mean "any limited liability company, limited liability partnership, corporation, sole proprietorship, association, or other group, however organized and regardless of whether operating for profit or not for profit, including a financial institution organized, chartered, or holding a license authorizing operation under the laws of this state, any other state, the United States, or any other country, that, alone or jointly with others, determines the purpose and means of processing personal data."[1] Businesses would not include Ohio public entities, political subdivisions or processors to the extent that the processor is acting in the role of a processor.[2]

Processors

Under OPPA, "Processors" would mean a natural or legal person who processes personal data on behalf of a business subject to OPPA.[3] With respect to determining whether a person acts as a "business" or a "processor," OPPA would set forth that this it a fact-based determination dependent on the context in which the personal data is processed.[3]

Consumers

Under OPPA, consumers would mean a "natural personal who is a resident" of Ohio "acting only in an individual or household context." Consumers would not include people acting in a "business capacity" or employment context, such as contractors, job applicants, directors, officers or owners.[5]

[1] Ohio Personal Privacy Act, Sub. H. B. No. 376, 134th General Assembly
[2] Id.
[3] Id.
[4] Id
[5] Id.

New Data Processing and Notice Requirements, Emerging Consumer Rights, and Cybersecurity Programs

If enacted, OPPA would require businesses to adopt a transparent and consumer-focused method of processing personal data. Specifically, under OPPA, businesses would be required to communicate certain core aspects of the way that the business interacts with personal data through conspicuous posting of

a privacy policy. Moreover, if Ohio enacts OPPA, it will join an expanding group of other U.S. states in providing residents with specific rights pertaining to their personal data, such as the rights to request a copy, correction, or deletion of their personal data.

Meanwhile, through Ohio's DPA, Ohio has already joined other U.S. jurisdictions in setting forth parameters for cybersecurity programs. That said, Ohio has taken the unique approach through its DPA of framing the cybersecurity program as an incentive-based eligibility criteria for an affirmative defense as opposed to a requirement enforced through punitive measures.

5.1. OPPA Privacy Policy Requirement

Under OPPA, businesses would be required to provide consumers notice about the personal data that it processes about the consumer. Notice would be in the form of a conspicuously posted privacy policy that would identify:

- the categories of personal data processed by the business;
- the purposes of processing for each category of personal data;
- the categories of sources from which the personal data is collected;
- the categories of processors with whom the business discloses personal data;
- the data retention practices and the purposes for retention;
- ·how individuals can exercise their rights under OPPA;
- how the business will notify consumers of material changes to its privacy policies;
- the categories of any third parties to whom the business sells personal data (if any); and
- · the identities of any affiliates to which personal data may be transferred[1]

5.2. New Consumer Rights Under OPPA

If enacted, OPPA would provide consumers specific rights with respect to the processing and

[1] Id.

maintenance of their personal data. Businesses would be prohibited under OPPA from discriminating against consumers who choose to exercise these rights, such as charging such individuals different prices or rates for goods or services. [1] Processors would be required to assist businesses in responding to consumer requests.[2]

Consumer Right to Request Copy of Personal Data

If enacted, OPPA would mirror existing U.S. comprehensive data privacy legislation in providing consumers the right to request a copy of their personal data that the consumer previously provided to a business. Under the proposed framework, businesses would not be obligated to provide access to a consumer's personal data more than once in a twelve-month period.[3]

Consumer Right to Request Correction of Personal Data

Additionally, if enacted, OPPA would provide consumers the right to request the correction of inaccuracies in the consumer's personal data and businesses would be required to correct any such inaccuracies.[4] A similar right exists in existing comprehensive data privacy legislation in the U.S. and abroad (such as the "right to rectification" under Article 16 of the EU General Data Protection Regulation ("GDPR")).

Consumer Right to Request Deletion of Personal Data

Under OPAA, a consumer's right to request the deletion of their personal data maintained by a business would also be protected. Businesses would be required to comply with deletion requests with limited exceptions, such as the event in which the personal data is necessary for the business to adhere to its written records retention schedule. [5]

Consumer Right to Prevent Sale of their Personal Data

If enacted, OPPA would also provide consumers the right to request a business not to sell the consumer's personal data or process the consumer's personal data for the purpose of targeted advertising.[6] Moreover, businesses that sell personal data or that use processed personal data for the purposes of targeted advertising would be required to provide notice of these facts in a manner to enable consumers to "opt out" of the sale of their personal data and/or the use of their personal data for targeted advertising.[7]

5.3. Cybersecurity Programs Under the Ohio DPA

Under the Ohio DPA, covered entities that are seeking an affirmative defense are required to create, maintain, and comply with a written

[1] Id.
[2] Id.
[3] Id.
[4] Id.
[5] Id.
[6] Id.
[7] Id.

cybersecurity program that (1) contains administrative, technical and physical safeguards for the protection of personal information and that (2) reasonably conforms to an industry recognized cybersecurity framework.[1]

Ohio's DPA notes that the cybersecurity program shall be designed to protect the security of personal information, protect against anticipated threats to the security or integrity of the information, and protect against unauthorized access the personal information.[2] The DPA notes that the scale and scope of a cybersecurity program is appropriate if based on factors such as (1) the size and complexity of the covered entity, (2) the sensitivity of the information to be protected, (3) the nature and scope of the activities of the covered entities, and (4) the resources available to the covered entity.[3]

"Industry recognized" cybersecurity frameworks to which a cybersecurity program may conform include:

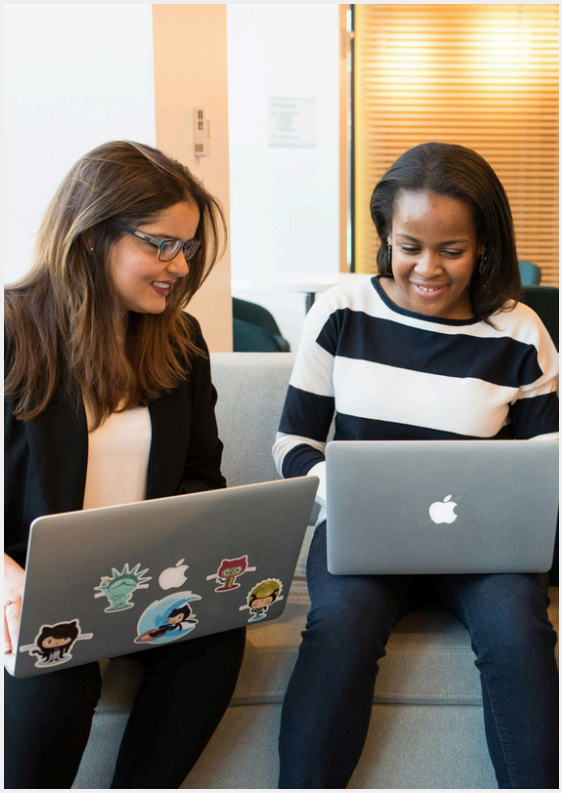
- National Institute of Standards and Technology's (NIST) framework for improving critical infrastructure cybersecurity;
- NIST Special Publication 800-171;
- NIST Special Publications 800-53 and 800-53a;
- The Federal Risk and Authorization Management Program's (FedRAMP) Security Assessment Framework;
- The Center for Internet Security Critical Security Controls for Effective Cyber Defense; or
- International Organization for Standardization / International Electrotechnical Commission's 27000 Family – Information Security Management Systems[4]

[1] Ohio Rev. Code, 1354.02(A)(1)-(2)
[2] Ohio Rev. Code, 1354.02(B)(1)-(3)
[3] Ohio Rev. Code, 1354.02(C)(1)-(5)

5.4. New Data Protection Requirements Under OPPA

Under OPPA, processors would be required to maintain "reasonable" administrative, technical, and physical safeguards to protect the security and confidential of personal data.[5] OPPA notes that safeguards

[4] Ohio Rev. Code, 1354.03(A)(1)
[5] Ohio Personal Privacy Act, Sub. H. B. No. 376, 134th General Assembly



shall reflect the nature and scope of the activities of the processor and its role in possessing the personal data.[1] Unlike other privacy legal frameworks such as HIPAA that require covered entities to implement administrative, technical, and physical safeguards, OPPA does not narrowly specify the applicable safeguards, which presumably may entail actions such as monitoring of information systems, employee training on cybersecurity, or requirements with respect to implementation of policies/procedures beyond the core privacy policy.

5.5. Data Processing of Minors' Data

Under OPPA, businesses would be prohibited from selling the personal data collected online of a known child without complying with the requirements or exceptions of the Children's Online Privacy Protection Act of 1998 (COPPA).[2] This requirement mirrors comprehensive data privacy legislation in other jurisdiction, such as Connecticut and other jurisdictions that afford special protections to the personal data of minors.

[1] Id.
[2] Id.

OPPA Enforcement

Unlike similar legislation in other jurisdictions, OPPA does not establish a new privacy regulator. If enacted in its current form, the Ohio Attorney General would maintain exclusive authority to enforce OPPA through investigation of businesses and processors for compliance and civil penalties of up to five thousand dollars for each violation.[3]

If the attorney general has reasonable cause to believe that a business or processor has engaged or is engaging in an act or practice that violates OPPA, the attorney general would be able to bring an action in an Ohio court of common pleas to seek relief in the form of declaratory judgements that the business/processor has engaged in an act or practice that violates OPPA as well as injunctive relief (both preliminary and permanent) to prevent further violations and compel compliance.[4]

[3] Id.
[4] Id.

Conclusion

Ohio is advancing toward a data protection landscape in which it simultaneously promotes and requires the safeguarding of personal data of its residents through collective legislation based in both incentives and requirements. At the aggregate level, Ohio's data protection legislation is focused on rewarding businesses for taking steps to enhancing their cybersecurity posture while also affording consumers newfound control over their personal information and imposing requirements of companies with respect to data processing.

Through enacting an incentive-based DPA, Ohio took the bold and unprecedented step in rewarding businesses that focus on enhancing their cybersecurity postures. That said, an incentive-based program has limitations. Through OPPA, Ohio would round out its data protection legislation by mirroring recent and similar legislation across the U.S. in affording consumers with specific rights pertaining to the handling of their personal data, requiring the declaration of practices pertaining to processing of personal data through the posting of a privacy policy, as well as requiring the maintenance of administrative, technical, and physical safeguards.

Contact Us

+1 (216) 348-5400
https://www.mcdonaldhopkins.com/
jgiszczak@mcdonaldhopkins.com
600 Superior Avenue E., Suite 2100
Cleveland, Ohio 44114-2653 USA