Insights, News & Events

MARYLAND SET TO ENACT RIGID DATA PRIVACY LAW: WHAT EMPLOYERS NEED TO KNOW BEFORE OCTOBER 2025 EFFECTIVE DATE

Insights
May 15, 2024

Maryland lawmakers recently passed comprehensive consumer privacy legislation that, in some ways, is stronger than laws seen in other states and even a key bill proposed by Congress. Governor Wes Moore signed the Maryland Online Data Privacy Act (MODPA) on May 9, which means businesses in the state will need to begin compliance work before the October 1, 2025, effective date. With its emphasis on data minimization and more rigid requirements than in the pending federal privacy bill, you'll still have plenty of work to do before then. Here is what employers need to know about MODPA.

Who Does MODPA Apply To?

MODPA applies to a person that "conducts business" in Maryland, or provides products or services that are targeted to Maryland residents and who, during the preceding year:

- controlled or processed the personal data of at least 35,000 Maryland consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or
- controlled or processed the personal data of at least 10,000 Maryland consumers while deriving more than 20% of gross revenue from the sale of personal data.

Several entities are exempt from the requirements under MODPA. This includes certain nonprofits, financial institutions, and state government entities. Unlike some other state privacy laws, however, Maryland's proposed law

Related People

Monica Snyder Perl
Partner
617.532.9327

Service Focus

Consumer Privacy Team

Privacy and Cyber

Related Offices

Baltimore

does not provide a blanket exemption for nonprofits or institutions of higher education. It also does not contain an entity-level exemption for HIPAA-covered entities.

Within the definition of a "consumer," the law also excludes Maryland residents that are acting in a commercial or employment context. This means businesses are not subject to the law if they are handling personal information strictly in a business-to-business context. **Critically, it also means that employers do not have to extend privacy rights in the employment context.** In the United States, only California's Consumer Privacy Rights Act (CPRA) goes as far as extending its privacy protections to the employment context.

Heightened Data Minimization Requirements

MODPA imposes heightened data minimization requirements based on whether the data at issue is personal or sensitive. It restricts the collection of personal data to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains.

For sensitive data, the data minimization expectations are even more stringent. MODPA prohibits the sale of sensitive data concerning consumers unless it is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the data pertains. The law defines sensitive data to include data revealing racial or ethnic origin; religious beliefs; consumer health data; sex life; sexual orientation; status as transgender or nonbinary; national origin; and citizenship or immigration status.

It also includes genetic and biometric data, personal data of a consumer who the controller knows or has reason to know is a child, and precise geolocation data. MODPA does not define or provide guidance as to what exactly constitutes "reasonably necessary" or "strictly necessary."

Consumer Rights

MODPA further provides consumers with rights found in many other state comprehensive privacy laws – such as Kentucky, Virginia, California, Connecticut, Colorado, Utah, Delaware, Indiana, Iowa, New Hampshire, New Jersey, Montana, Oregon, Tennessee, and Texas.

These rights include, but are not limited to:

- confirming whether a controller is processing the consumer's personal data;
- correcting inaccuracies in the consumer's personal data;
- deleting personal data provided by, or obtained about, the consumer unless retention of the personal data is required by law;
- obtaining a copy of the consumer's personal data processed by the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to easily transmit the data to another controller without hindrance;
- obtaining a list of the categories of third parties to which the controller has disclosed the consumer's personal data, or a list of the categories of third parties to which the controller has disclosed any consumer's personal data, if the controller does not maintain this information in a format specific to the consumer; and
- opting out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

Restrictions for Processing and Sale of Minors' Data

For consumers under 18 years old, MODPA prohibits the sale, or processing for purposes of targeted advertising, of personal data if the controller knew, or should have known, that the consumer is under 18. This prohibition is strict compared to other laws that require actual knowledge of a consumer's age or provide an opportunity for consumers to opt-in for the processing and sale of minors' data.

Data Protection Assessments

MODPA also requires data protection assessments for processing activities that involve targeted advertising, the sale of personal data, profiling in limited circumstances, and the processing of sensitive data, to name a few. Under Maryland's law, controllers must regularly conduct and document a Data Protection Assessment for each of their "processing activities that present a heightened risk of harm to a consumer," including an assessment for each algorithm that is used.

Processing activities that present a heightened risk of harm to a consumer include:

- the processing of personal data for the purposes of targeted advertising;
- the sale of personal data;
- the processing of sensitive data; and
- the processing of personal data for the purposes of profiling in which the profiling presents a reasonably foreseeable risk of:
  - unfair, abusive, or deceptive treatment of a consumer;
  - having an unlawful disparate impact on a consumer;
  - financial, physical, or reputational injury to a consumer;
  - a physical or other intrusion upon the solitude or seclusion or the private affairs or concerns of a consumer if the intrusion would be offensive to a reasonable person; or
  - other substantial injury to a consumer.

Anti-Discrimination

MODPA further prohibits, with limited exceptions, the collection, processing, or transferring of personal data or publicly available data in a manner that unlawfully discriminates in, or otherwise unlawfully makes unavailable, the equal enjoyment of goods or services on the basis of various categories. These include race, color, religion, national origin, sex, sexual orientation, gender identity, or disability, unless the collection, processing or transfer of personal data is for specific purposes, such as for the controller's self-testing to prevent or mitigate unlawful discrimination.

Enforcement

Maryland's Division of Consumer Protection will be tasked with enforcing MODPA under the Attorney General. Violations of the law will be treated as unfair, abusive, or deceptive trade practices subject to enforcement and penalties under Maryland's Consumer Protection Act. The law provides a 60-day cure period to controllers and

processors upon receipt of a notice of a violation. MODPA will not have any effect on or application to any personal data processing activities before April 1, 2026.

What Should Businesses Do to Prepare?

Although October 1, 2025, may seem like a long way away, compliance steps to get in line with data privacy laws can take time. If your business will be subject to this new law, you may want to consider taking these steps sooner rather than later:

- Evaluate your organization's current data collection and privacy procedures;
- Compile a record of historical consumer data your organization has collected;
- Deliberate on potential future consumer data collection avenues;
- Identify data your organization may gather concerning minors;
- Craft protocols for addressing consumer inquiries; and
- Work with data privacy counsel to ensure that your organization will be able to comply with the law.

Conclusion

For further information, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on the firm's Consumer Privacy Team, or the Privacy and Cyber Practice Group. Fisher Phillips will continue to monitor consumer privacy law developments and will provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox.