PUBLICATION

Maryland Enacts Comprehensive Consumer Privacy Legislation: What You Need to Know

May 09, 2024

Maryland Governor Wes Moore signed the Maryland Online Data Privacy Act of 2024 (MODPA) into law on May 9, 2024. This new law establishes transparency, assessment, and consumer rights requirements for organizations that fall within its scope, and much like the state laws that have come before it, the MODPA includes its own unique provisions that will add additional complexities to an organization's compliance efforts and data use strategy.

Although the MODPA takes effect October 1, 2025, it does not "have any effect on or application to any personal data processing activities before April 1, 2026," giving organizations critical time to put the nuances of the law into practice. However, this extended time should not be viewed as a license to delay decision-making, as the obligations of the law will take time for organizations to implement. Read more to learn about how the MODPA may affect your business and what you can do now to prepare for its arrival.

To whom does the MODPA apply?

The thresholds of the MODPA are lower than those of many other state comprehensive privacy laws, making it more likely that organizations will be subject to the new law.

The MODPA applies to organizations that: (i) conduct business in Maryland; or (ii) provide services or products that are targeted to Maryland residents, and, during the immediately preceding calendar year, either:

- 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** and derived **more than 20 percent** of their gross revenue from the sale of personal data.

The law includes data-level exemptions similar to other state laws, including, among others: Protected Health Information processed under the Health Insurance Portability and Accountability Act (HIPAA); personal data regulated by the Fair Credit Reporting Act; and personal data regulated by the Family Educational Rights and Privacy Act (FERPA).

However, the law includes few entity-level exemptions. Such exemptions are limited to:

- Regulatory, administrative, advisory, executive, appointive, legislative, or judicial bodies or instrumentalities of the state of Maryland;
- National securities associations registered under the Securities Exchange Act of 1934 or registered futures associations under the Commodity Exchange Act;
- Financial institutions or affiliates subject to the Gramm-Leach-Bliley Act (GLBA); and
- Non-profit organizations that process or share personal data solely to assist law enforcement in investigating insurance-related criminal or fraudulent acts or first responders to catastrophic events.

What is "personal data?"

The MODPA follows a definition of personal data similar to the majority of other states. "Personal data" means any information that is linked or can be reasonably linked to an identified or identifiable consumer. Personal data does not include de-identified data or publicly available information.

"Sensitive data" includes:

- Racial or ethnic origin, religious beliefs, consumer health data, sex life, sexual orientation, status as transgender or nonbinary, national origin, or citizenship or immigration status;
- Genetic data or biometric data;
- Personal data of a consumer that the controller knows or has reason to know is a child under 13 years of age; and
- Precise geolocation data (identifying a consumer's location within a radius of 1,750 feet).

This definition reflects a view of sensitive data similar to that of other state laws, but with a nuance concerning: (i) consumer health data; and (ii) biometric and genetic data.

- Under the MODPA, consumer health data includes personal data the controller actually *uses* to identify a consumer's physical or mental health status, rather than information "reasonably linkable" to a consumer's health as defined in sectoral consumer health data laws such as Washington's My Health My Data Act.
- Under the MODPA, biometric or genetic data is considered sensitive data regardless of whether it is "processed for the purpose of uniquely identifying an individual" as limited by other comprehensive privacy laws.

What obligations do subject entities have?

Controllers subject to the MODPA are required to:

- Provide consumers with a reasonably accessible, clear, and meaningful privacy notices including the disclosures required by the MODPA, which are similar to those required under other state privacy laws;
- Limit 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;
- Process personal data only for a purpose reasonably necessary to or compatible with the purposes disclosed to the consumer, unless with the consumer's prior consent;
- Provide an effective mechanism for a consumer to revoke the consumer's consent;
- Collect, process, or share sensitive data only where strictly necessary to provide or maintain a specific product or service requested by the consumer;
- Not sell sensitive data;
- Not process personal data in violation of state or federal laws that prohibit unlawful discrimination;
- Not sell the personal data of a consumer without the consumer's consent if the controller knew or should have known the consumer is under 18 years of age;
- Not discriminate against consumers for exercising their consumer rights under the law;
- Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data; and
- Perform data protection assessments for processing activities that present a heightened risk of harm.

Maryland's prohibition on: (i) the sale of sensitive data; and (ii) collection and processing except as strictly necessary to provide a product or service to the consumer, is one of the most restrictive to date, and requires particular consideration for organizations in their use of cookies and other tracking technologies due to the broad interpretation of what is considered a "sale" under state privacy laws similar to the MODPA.

What rights do individuals have?

Like other state privacy laws to date, the MODPA provides consumers certain rights. Note, that the definition of "consumers" is limited to residents of Maryland and does not include individuals acting in a business or employment context.

Consumers have the right to:

- Confirm whether a controller is processing the consumer's personal data, and access such data if so;
- Correct inaccuracies in the consumer's personal data;
- Require a controller to delete personal data provided by, or obtained about, the consumer unless retention of the personal data is required by law;
- Data portability when data processing is done through automated means;
- Obtain a list of the categories of third parties to which the controller has disclosed the consumer's personal data;
- Opt out of: (i) targeted advertising; (ii) the sale of personal data; and (iii) profiling in furtherance of automated decisions that produce legal or similarly significant effects concerning the consumer; and
- Appeal rights requests that have not been fulfilled.

With each state privacy law introduced, organizations must reevaluate the core principles of their privacy programs, as well as the nuanced measures required by variations in this myriad of laws. Regardless of where an organization is located, consideration of the MODPA and other state privacy laws can better position your organization to navigate the rapidly changing privacy environment while aligning with your core business objectives.

For assistance in assessing your organization's strategic data goals and compliance readiness under the MODPA or other U.S. state privacy laws, please contact any member of Baker Donelson's Data Protection, Privacy and Cybersecurity team.