Maryland Lands On Novel Data Privacy Scheme

On May 9, Maryland Governor Wes Moore's signing of the Maryland Online Data Privacy Act (MODPA) made Maryland the eighteenth state to enact comprehensive data privacy legislation. MODPA does not closely track any existing data privacy laws but pulls concepts from the draft Washington Privacy Act (WPA) (which has yet to pass the legislature), Washington's My Health My Data Law (MHMD), and Connecticut's consumer health privacy law, while also attempting several novel approaches.

MODPA's original approach to data privacy, which includes potentially ambiguous language, will likely require additional compliance analysis for businesses using sensitive data, such as consumer health data in Maryland. MODPA takes effect October 1, 2025, but only has effect on and applies to data processing activities after April 1, 2026.

Applicability Thresholds and Exemptions

MODPA applies to entities that conduct business in Maryland or produce products or services targeted to Maryland residents and, in one year, control or process the personal data of either:

- 35,000 consumers (excluding personal data controlled or processed solely for the purpose of completing a payment transaction).
- 10,000 Maryland consumers and derives more than 20% of its gross revenue from the sale of personal data.

MODPA's applicability thresholds are relatively low—the lowest per-capita threshold of any general state data privacy law so far other than Texas (which has none).

While MODPA contains data-level exceptions for protected health information under HIPAA and information subject to the Family Educational Rights and Privacy Act (FERPA) and Gramm-Leach-Bliley Act (GLBA), it does not exclude at the entity level nonprofits (nonprofits that process or share personal data to assist law enforcement or first responders are excluded), institutions of higher education, or HIPAA-covered entities.

New Obligations for Controllers: Sensitive Data Sale Prohibition and Data Minimization

MODPA separates itself from other state's data privacy laws with its comprehensive prohibition on the sale of sensitive data and its stringent commitment to data minimization.

Controllers are completely prohibited without exception (e.g., by obtaining informed consent) from selling sensitive data, which is defined as any of the following:

- Data revealing racial or ethnic origin, religious beliefs, sex life, sexual orientation, status as transgender or non-binary, national origin, or citizenship or immigration status.
- Consumer health data (defined as data that a controller uses to identify a consumer's physical or mental health status).
- Genetic or biometric data.
- Personal data of a consumer that is known or the controller has reason to know is a child.

- Precise geolocation data.

Notably, the definitions for "Genetic Data" and "Biometric Data" in MODPA are much broader than those definitions in other state privacy statutes except for Oregon's, which is similar. Under MODPA's definition, Genetic and Biometric Data do not have to be actively used to identify consumers in order to qualify, but rather the definition includes any data that *could* be used to identify consumers.

Entities that are selling sensitive data under a consent model will need to consider whether the Maryland law is applicable and, if so, how to cease the sale of sensitive data from at least Maryland consumers.

Controllers are also required to adhere to stricter data minimization principles. For sensitive data, controllers may only collect sensitive data where it is "strictly necessary to provide or maintain a specific product or service requested by the consumer," and for personal data generally, controllers may only collect "what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the customer." These principles differ from other state's data minimization principles in that processing is limited to what is necessary for the "service requested by the customer" rather than the stated purpose of processing. Controllers complying with other state privacy laws' minimization principles will need to evaluate whether their current purposes of processing are limited to what is necessary and/or proportionate to the service they are providing a consumer.

Aside from these innovations, MODPA largely tracks the WPA and Connecticut's consumer health data privacy law for controller obligations. Similar to the WPA, controllers under MODPA must conduct data protection assessments, establish processes for responding to consumer requests and appeals, maintain reasonable data security practices, provide a privacy notice, and provide a method for opt-outs (although recognition of universal opt-out mechanisms is optional if a clear and conspicuous opt-out link is available).

MODPA's data protection assessment obligation also includes a new requirement. Controllers must assess each algorithm they use in high-risk processing activities. High-risk activities include the following:

- Processing personal data for the purpose of targeted advertising.
- Sale of personal data.
- Processing of sensitive data.
- Processing that poses a reasonably foreseeable risk of unfair, abusive, or deceptive treatment of a consumer; unlawful disparate impact on a consumer; or financial, physical or reputational damage.

"Algorithm" is undefined in the statute, so businesses will need to evaluate on a case-by-case basis whether the processing tools they use qualify as an algorithm and monitor regulatory guidance.

MODPA's consumer health data obligations are rather few, similar to Connecticut's law, only imposing confidentiality obligations on employees touching consumer health data and prohibiting geofencing around certain health institutions.

Consumer Rights

MODPA includes a typical list of consumer rights (similar to the WPA with one addition), including the rights for consumers to:

- Confirm if a controller is processing their data.
- Access their data and obtain a copy.
- Correct their data.
- Require the controller to delete their personal data.
- Opt out of processing for the purposes of targeted advertising, sale of personal data, or profiling in furtherance of solely automated decisions that produce significant effects.
- Obtain a list of third parties to whom personal data is disclosed.

Children's Data

MODPA contains new protections related to children's data as well. MODPA prohibits the following actions:

1. The processing of personal data for the purposes of targeted advertising.
2. The sale of personal data if the controller "knew or should have known" that the consumer is under the age of 18.

The "know or should have known" standard differs from the standard for recognizing children's data under Florida's and California's data privacy laws and may require greater diligence from companies to determine whether the data they are collecting belongs to someone under the age of 18. Once again, businesses may need to evaluate their data processing environments on a case-by-case basis and monitor regulatory guidance for information on how to meet this standard.

Enforcement

There is no private right of action under MODPA, as it is enforceable exclusively by the Maryland Attorney General. There is a 60-day cure period for violations at the discretion of the Attorney General until April 1, 2027. If the controller or processor fails to cure the alleged violation within 60 days, the Attorney General may initiate an enforcement action and may collect up to $10,000 per violation (and up to $25,000 per subsequent violation).

Important Dates

- **October 1, 2025**: MODPA goes into effect.
- **April 1, 2026**: MODPA begins applying to personal data processing activities.
- **April 1, 2027**: End of the discretionary cure period.

If you have any questions about MODPA or other state data privacy rules, please contact the authors.