DAVIS GILBERT

Privacy, Technology + Data Security

The Maryland Online Data Privacy Act: Familiar Requirements, but Stricter Sensitive Data Mandates

The Bottom Line

- Maryland is about to become the 17th state to enact a comprehensive consumer privacy law.
- While some aspects of the Maryland Online Data Privacy Act are consistent with the existing state comprehensive consumer privacy laws, there are stringent limitations surrounding sensitive data, including a first-of-its-kind prohibition on selling sensitive data.
- Covered businesses that handle sensitive data and do business in Maryland should revisit their compliance programs.

Maryland's Legislature passed the Maryland Online Data Privacy Act of 2024 (MODPA) on April 6, 2024. While MODPA carries many similarities to other comprehensive state data privacy laws, it has some stricter parameters around the sharing of sensitive data.

Pending Governor Wes Moore's signature, MODPA will go into effect on October 1, 2025, although it will not "have any effect on or application to any personal data processing activities before April 1, 2026."

Threshold Requirements

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

- 35,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction or
- 10,000 consumers and derive more than 20% of revenue, or receive a discount on, the price of any goods or services, from the sale of personal data.

Both of these triggering scenarios are considerably lower than most other state consumer privacy laws, except for the recently passed New Hampshire Privacy Act. The exclusion of payment transactions (which can also be found in other privacy laws like Connecticut's, Oregon's and Montana's), benefits retailers and other small businesses that only use credit and debit card information to facilitate sales.

Alignment with Existing State Laws

Like other state privacy laws, MODPA provides consumers with a series of rights regarding their personal data: rights of access, correction, deletion and data portability. Consumers would also have the right to opt out of targeted advertising, sales of personal data and profiling "in furtherance of decisions that produce legal or similarly significant effects concerning the consumer." The 45-day timeline for responding to consumer requests, with the option to obtain a 45-day extension, is also the same.

MODPA also provides similar definitions of "consumer" and "personal data," and the list of exempt entities is consistent with other state laws.

For companies whose processing activities involve targeted advertising, the sale of personal data, profiling (in limited circumstances) or the processing of sensitive data, MODPA requires data protection assessments.

Data Minimization and Restrictions on Sensitive Data

While almost every comprehensive privacy law – from the GDPR to each U.S. state law – includes the principle of data minimization, meaning controllers should limit their collection of personal data to what is directly relevant and necessary to accomplish a specified purpose – MODPA goes much further. It restricts companies from collecting, processing or sharing sensitive data entirely, except where *"strictly necessary to provide or maintain a specific product or service requested by the consumer."*

Most significantly, MODPA contains a blanket prohibition on selling sensitive data, which is the first of its kind under any state privacy law. This unique aspect of the law will require covered businesses that sell and share sensitive data to adjust their compliance programs and could have far-reaching consequences for companies that operate in non-HIPAA-regulated health care space or deploy website tracking technologies.

MODPA defines "sensitive data" similarly to other state laws, but adds a twist on Consumer Health Data, which it defines as "personal data the controller uses to identify a consumer's physical or mental health status." It explicitly includes data related to gender-affirming treatment

or reproductive or sexual health care. "Physical or mental health status" is not defined. To trigger the application of Consumer Health Data, a controller must actually be *using* the data to identify a consumer's health status. This goes beyond other laws, like Washington's My Health My Data Act, which simply covers personal information that identifies the consumer's past, present or future physical or mental health status.

Another variation on sensitive data from existing state laws (e.g. Virginia) is that it broadly includes any genetic or biometric data, regardless of whether the data is being used to uniquely identify a consumer.

Children and Teenagers

As with every comprehensive state privacy law to date, controllers under MODPA are required to process the data of children younger than 13 in accordance with the Children's Online Privacy Protection Act (COPPA). However, MODPA goes a step further than other state privacy laws and prohibits selling a consumer's personal data or using that data for purposes of targeted advertising if the controller *knew or should have known* that the consumer is under the age of 18. This is a particularly strict prohibition compared to other states that require opt-in consent from consumers between 13 to 15 years old (e.g. California, Connecticut, Oregon and Montana), or that require *actual* knowledge of a consumer's age.

Enforcement

MODPA is enforceable solely by the Maryland Attorney General. Although it does not specifically provide consumers with a private right of action, it does not prevent consumers from pursuing remedies provided by other laws. Violations of the MODPA are considered unfair, abusive or deceptive trade practices under Maryland's Consumer Protection Act.

For the first 18 months from the law's effective date, the Attorney General may issue companies a notice of violation and grant them 60 days to cure such violation before bringing an enforcement action. The law's notice-and-cure period sunsets on April 1, 2027.

If the controller or processor fails to remedy the issue within the 60-day cure period, the Attorney General can initiate an enforcement action. Penalties can be up to $10,000 per violation. But, if the fine is in connection with a repeat violation, it may cost up to $25,000 for each violation.

For More Information

Please contact the attorneys listed below or the Davis+Gilbert attorney with whom you have regular contact.

Gary Kibel

Partner
212 468 4918
gkibel@dglaw.com

Jeremy Merkel

Associate
212 468 4976
jmerkel@dglaw.com