CLIENT ALERTS & INSIGHTS

REMINDER: Maryland Data Protection Law Comes into Effect on October 1st

SEPTEMBER 26, 2025

Key Takeaways

- Maryland's new data protection law, the Maryland Online Data Privacy Act (MODPA), takes effect October 1, 2025, and introduces stricter requirements for processing personal and sensitive data, especially for minors, compared to other state laws.
- Businesses should care because MODPA imposes heightened restrictions and prohibitions on the use of sensitive data and data of individuals under 18, increasing compliance obligations (beyond what is common under other U.S. state data protection laws) and the risk of enforcement actions by the Maryland Attorney General.
- To prepare, businesses operating in Maryland should review and update their data collection, processing, and privacy practices to ensure they only process data that is strictly necessary for requested products or services, obtain opt-in consent for sensitive data, and implement robust consumer rights request procedures.

Maryland's data protection law closely aligns to other omnibus U.S. state data protection laws but includes key nuances and enhanced requirements related to processing sensitive data and data minimization.

Well over a dozen U.S. states now have omnibus data protection laws in effect. On October 1, 2025, Maryland will join their ranks with the Maryland Online Data Privacy Act (the "MODPA").

The MODPA aligns in structure to many of the existing U.S. state data protection law. However, it will also usher in new, more restrictive requirements and prohibitions with respect to personal data processing. For example, a business's processing of any personal data must be reasonably necessary for the maintenance or provision of products or services the applicable consumer specifically requested.

The MODPA also ushers in new, more restrictive prohibitions relating to the processing of sensitive data and personal data relating to those consumers under the age of 18.

Below, see more details relating to the MODPA and key considerations for covered businesses. Additionally, see Benesch's and Data Meets World's interactive U.S. State Privacy Laws website page for a high level overview of what U.S. states have data protection laws on the books and of what such data protection laws cover and will require.

Scope and Applicability of Maryland Data Protection Law

All states set forth a prerequisite that only a business that operates or does business in the specific state is subject to the law. But it is not that simple. To be subject to the applicable state laws, the "do business in the state" prerequisite must be met, but a business must also meet certain "triggers".

Under U.S. state data protection laws, there are generally three triggers to consider: (1) annual gross revenue (not just the revenue derived out of the applicable state); (2) the total collection of personal data from consumers in the applicable state; or (3) the collection and sale of the state's consumers' personal data.

The MODPA will apply to any business operating or doing business in Maryland, and that meets one of the following thresholds:

- Annually processes 35,000 or more Maryland consumers' personal data (excluding personal data processes solely as necessary to complete a payment transaction); OR
- Derives 20% of its gross, worldwide annual revenue from selling personal data and annually processes 10,000 Maryland consumers' personal data.

Each state has taken a slightly different approach. For example, some states like Texas and Nebraska do not include ***any*** threshold triggers. California is still the only U.S. state omnibus data protection law that governs the processing of employee, job applicant, contractor, and business-to-business personal data

Maryland Data Protection Law Privacy Rights

Under the MODPA, consumers have the following rights to:

- to confirm whether a business is processing their personal data
- to correct their personal data
- to have their personal data deleted
- to receive a copy of the personal data held about them in a portable and usable form (data portability)
- to obtain a list of categories of third parties with whom their information was disclosed to or a list of categories of third parties with whom any consumer's information is disclosed to (if specific lists are not maintained)
- to opt-out of the sale of their personal data
- to opt-out of targeted advertising
- to opt-out of profiling through solely automated means in furtherance of decisions with legal or similar effect (e.g., employment, education, criminal justice, etc.)

The MODPA defines "sale" as the exchange of personal information for monetary **or other** purposes-which aligns with California's (and most other U.S. states') broad approach.

Additionally, in line with other omnibus U.S. state data protection laws, the MODPA requires businesses to give consumers the right to appeal that businesses denial of a data privacy right request.

Sensitive Data Under Maryland Law & Data Processing Prohibitions

Under the MODPA, businesses are prohibited from processing sensitive personal data without first obtaining the consumer's prior, opt-in consent. The MODPA defines "sensitive data" as including:

- race, ethnicity, national origin, and religion
- consumer health data
- sexual orientation and transgender or non-binary status
- citizenship or immigration status
- genetic or biometric data
- the personal information of a child (younger than 13)
- a consumer's precise geolocation (within a radius of 1,750 feet)

Regardless of consent, businesses are only permitted to collect and process sensitive data where the sensitive data is strictly necessary for providing or maintaining a specific product or service required by the applicable consumer. The MODPA prohibits all other uses or collection of sensitive data (including, without limitation, the sale of sensitive data).

The restrictions on processing sensitive data are unique to Maryland as many other U.S. state data protection laws permit the broad use of sensitive data assuming the business first obtains the applicable consumer's prior express consent.

Maryland has also led the way on U.S. states further restricting the use of personal data relating to consumers under the age of 18. Businesses subject to the MODPA are prohibited from (i) processing personal data for purposes of targeted advertising if the business knew or should have known the personal data related or relates to consumers under the age of 18; and (ii) selling personal data that relates to a consumer that the business knew or should have known is under the age of 18.

Maryland Data Minimization

In line with its restriction on the use of sensitive data, the MODPA also limits how businesses can collect and process personal data. Businesses must limit collection, processing, and sharing to what is reasonably necessary and proportionate to provide or maintain the specific product or service requested by the applicable consumer.

While all U.S. state data protection laws touch on data minimization-collecting and processing the minimum amount of data for specific purposes-they tend to permit processing so long as the processing is reasonably related to stated purposes under a business's applicable privacy notice.

The MODPA takes it a step further and restricts personal data process solely to products or services requested by the applicable consumer(s). While businesses may have some leeway in deciding what

is reasonably related to said products and services, businesses will need to carefully consider this data minimization principle and how it may affect their data processing activities.

Maryland Data Protection Law Enforcement

The MODPA does not provide individuals with a private right of action against businesses that violate the MODPA.

Instead of a private right of action, the Maryland state attorney general will have exclusive enforcement authority. For violations occurring on or before April 1, 2027, the Maryland Attorney General may provide a discretionary 60-day cure period.

Conclusion

As more states pass comprehensive data protection laws and such laws come into effect, more and more business will need to build out substantive data protection compliance programs.

Those programs need to be adaptable-as one business could be subject to multiple state laws and therefore must adapt to the nuanced differences-and will need to account for the different aspects of comprehensive data protection laws, such as (1) substantive privacy policies and notices; (2) consumer privacy right request policies and procedures; (3) reasonable, adequate technical, organizational, and physical security measures; (4) vendor and contract management programs to flow through required contractual provisions when engaging data processors and service providers; and (5) regular audit procedures and programs.

The above list is not exhaustive of all potentially applicable obligations; but it provides an example of the different requirements comprehensive data protection laws set forth.

Businesses that have not previously dealt with comprehensive data protection law compliance will need to invest a significant amount of time in developing the required policies and procedures. Additionally, even if businesses have previously dealt with other-or former versions of-comprehensive data protection laws, they will need to conduct comprehensive reviews to account for specific nuances and differences in the laws.

As more states continue to implement their own variations of data protection laws and business juggle the various requirements, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.