Articles + Publications | May 9, 2024

Maryland's New Privacy Law Shows More Teeth (But Not Necessarily Fangs)

WRITTEN BY

Kim Phan | Laura Hamady | Aileen Ng

On May 9, Maryland Governor Wes Moore signed the Maryland Online Data Privacy Act (MODPA) into law, making Maryland the 17th state to enact a comprehensive privacy law. Despite its name, MODPA's coverage is not limited to "online data." It applies to "personal data" collected in any manner, and strengthens the privacy protections beyond the models previously seen in other states.

The MODPA becomes effective on October 1, 2025.

Applicability

The MODPA has a broader scope, with lower applicability thresholds than seen in most states with comprehensive privacy laws, and is expected to cover more businesses. Specifically, the MODPA applies to controllers that conduct business in Maryland or provide products or services that are targeted to Maryland residents, and that during the calendar year:

(1) Control or process the personal data of at least **35,000 consumers**; or

(2) Control or process the personal data of at least **10,000 consumers** and derive more than **20% of its gross revenue** from the sale of personal data.

Stronger Data Minimization Requirement

Similar to other state privacy laws, the MODPA incorporates the concept of data minimization to limit the personal data a business collects and processes to what is reasonably necessary and proportionate to the stated purposes.

However, the MODPA contains specific language that strengthens the concept by restricting 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***." Accordingly, it is not sufficient for a business to merely disclose the purposes for which it collects personal data — the purposes must be tied to a specific product or service requested by the consumer. In other words, collecting personal data for any other purpose, for example, an internal business purpose, is prohibited.

With respect to "sensitive data" (which includes data revealing racial or ethnic origin, religious beliefs, consumer health data, genetic or biometric data, and precise geolocation, among others), the MODPA further limits the collection, processing, or sharing of sensitive data to what is "***strictly necessary***" to provide or maintain a specific product to service requested by the consumer. Thus, the typical exceptions to process sensitive data for business

©2026 Troutman Pepper Locke

purposes or with a consumer's consent are not available.

Sale of Sensitive Data Prohibited (With Exceptions)

Beyond the "strictly necessary" standard discussed above, the MODPA expressly prohibits the sale of sensitive data. Note, however, that the exceptions are couched in the definition of "sale of personal data" and provide an exclusion, in part, for when the consumer "directs the controller to disclose the personal data," which would require more than consent from a consumer.

Potential Opportunity (Not Right) to Cure

The MODPA provides businesses with a potential opportunity (not a right) to cure an alleged violation prior to the Maryland attorney general (AG) initiating an enforcement action. The factors the AG may consider in determining whether to grant a controller or processor a potential opportunity to cure include, among others: (1) the number of violations; (2) the size and complexity of the controller or processor; and (3) the extent to which the controller or processor has violated the MODPA or similar laws in the past. If such opportunity is granted, the cure period will be at least 60 days.

The discretionary cure period is only available for alleged violations occurring on or before April 1, 2027, which indicates that strict compliance is required after this date.

Enforcement and Remedies Under Maryland's UDAP Law

Following only Colorado, Connecticut, and New Hampshire, the MODPA expressly provides that a violation of the MODPA constitutes an unfair, abusive, or deceptive (UDAP) trade practice, which makes a privacy violation subject to some of the strongest consumer protection remedies and penalties available to the Maryland AG under the state's UDAP law, such as, increased civil and criminal penalties. However, the MODPA expressly carves out a consumer's private right of action, which is otherwise available for a UDAP violation.

Incorporating Maryland's UDAP law, each violation may incur a civil penalty of up to $10,000 for each violation, and up to $25,000 for each repeated violation. In addition to civil penalties, a person who commits a UDAP violation is guilty of a misdemeanor and is subject to a fine of up to $1,000 or imprisonment of up to one year, or both.

Consumer Rights

As provided in other state privacy laws, the MODPA provides consumers with specified privacy rights, requiring controllers to:

1. Confirm whether they process a consumer's personal data;

2. Correct inaccuracies to personal data;

3. Delete personal data;

4. Obtain a copy of personal data;

5. Allow consumers to obtain a list of the categories of third parties to which their personal data has been

disclosed; and

6. Allow consumers to opt out of the processing of personal data for: (a) targeted advertising; (b) sale of personal data; or (c) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects.

Exemptions

Similar exemptions are available under the MODPA which excludes the personal data of employees and personal data collected in the business-to-business context. Financial institutions are also exempt, as well as data that is subject to the federal Gramm-Leach-Bliley Act. Other data-level exemptions include protected health information, and personal data collected, maintained, disclosed, sold, communicated, or used as authorized under the federal Fair Credit Reporting Act.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber