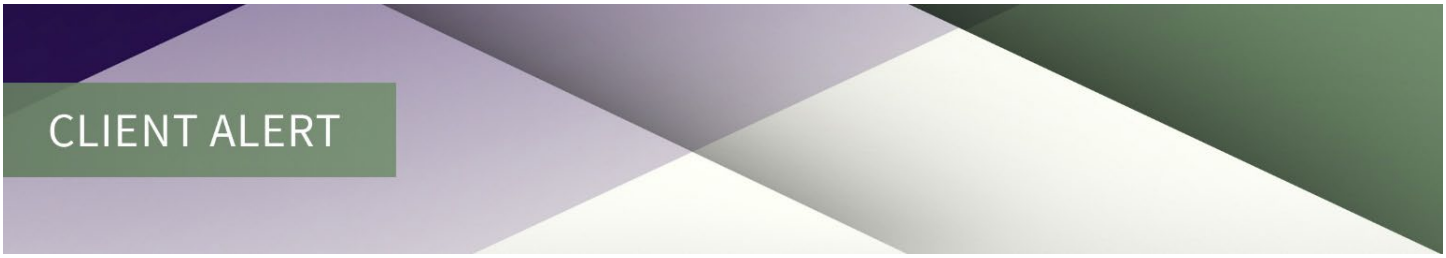

Maryland Enacts One of the Strictest Privacy Laws in the Nation

May 10, 2024

AUTHORS

Daniel K. Alvarez | Laura E. Jehl | Susan Rohol | Stefan Ducich
Michelle Bae

On May 9, 2024, Maryland Governor Wes Moore signed the Maryland Online Data Privacy Act of 2024 (the "MODPA") into law,[1] making Maryland the seventeenth state to enact comprehensive data privacy legislation. In several respects, the MODPA takes an approach similar to that of existing state privacy laws, but it includes several obligations that are more aggressive than these existing laws. These include: (1) imposing the strictest data minimization obligations and use restrictions under U.S. state privacy laws; (2) prohibiting the "sale" of sensitive data with very limited exceptions; and (3) prohibiting targeted advertising to children under the age of 18. These new obligations will pose strategic and tactical challenges for many businesses—from assessing how to modify their privacy programs to bring them into compliance (e.g., whether to apply these stricter requirements across all of the U.S. or just Maryland), to revising their privacy notices in ways that remain understandable, concise, and accessible. Moreover, the Maryland Attorney General's Office has enforcement authority, with statutory penalties of up to $10,000 for each violation (and up to $25,000 for each subsequent violation for repeated violations).

The MODPA will take effect on October 1, 2025; it does not have retroactive effect.

[1] Maryland Online Data Privacy Act of 2024, available here.

The MODPA Basics

Scope

As with a number of other comprehensive privacy laws, the MODPA employs many concepts similar to the EU General Data Protection Regulation ("GDPR"), such as the data controllers and processors construct. It imposes obligations with respect to consumer personal data collected by entities that conduct business in or target services to Maryland, and establishes rights for Maryland consumers with respect to their personal data, including the right to access, correction, deletion, and to opt out of sales. These obligations apply primarily to data controllers, which must execute contracts with the entities processing personal data on their behalf. However, unlike laws such as the California Consumer Privacy Act, as amended (the "CCPA"),[2] in which many obligations for service providers or other third-party processors are grounded in contract, the MODPA includes important data protection obligations (e.g., maintaining reasonable security measures and reducing reasonably foreseeable risks of harm to consumers) that also apply *directly* to both controllers and processors. Thus, non-compliance may open a processor to enforcement action by the Maryland Attorney General in addition to claims for damages by a controller stemming from the processor's breach of contractual obligations.

Application

The MODPA has a relatively low threshold requirement for a business to be subject to the law. It applies to a business that controls or processes the personal data of at least: (i) 35,000 Maryland consumers; or (ii) 10,000 Maryland consumers, and derives more than 20% of its gross revenue from the sale of personal data. By contrast, comparable thresholds under the Colorado Privacy Act ("CPA")[3] and the CCPA apply to businesses that control or process the personal data of 100,000 consumers (Colorado); or that buy, sell, or share the personal information of 100,000 consumers, or derive more than 50% of annual revenue from the sale of such data (California).

Exceptions

Like most other state privacy laws, the MODPA does not apply to business-to-business contact information or employee data, and certain entities and data types subject to other applicable privacy laws also are exempted from the MODPA. For instance, the MODPA provides an entity-level exemption for financial institutions subject to the privacy and data security requirements of the Gramm-Leach-Bliley Act. It also provides data-level exemptions for entities regulated under Maryland's state Insurance Article (with respect to personal data collected in furtherance of the business of insurance) and for protected health information subject to the Health Information Portability and Accountability Act.

[2] Cal. Civ. Code §§ 1798.100-199.
[3] Colo. Rev. Stat. §§ 6-1-1301, *et seq*.

Key Distinctions from Existing State Privacy Laws

The MODPA includes a number of differences from other state laws that are likely to have significant practical implications for how national—or even regional—companies operate with respect to the data they collect and use. Specifically:

- Strict Data Minimization and Use Limitation Requirements. Under the MODPA, controllers must 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* to whom the data pertains." (Emphasis added). Moreover, the processing of personal data is permissible under MODPA only where it is "reasonably necessary and proportionate" in relation to identified purposes—e.g., to provide a specifically requested product or service, take steps at the request of a consumer to enter into, or perform under a contract to which the consumer is a party.

  The MODPA does not offer any additional details as to what "reasonably necessary and proportionate to provide or maintain a specific product or service" entails, but this provision is significantly more robust than other state laws in narrowing the scope of personal data that controllers can collect. For example, in its recently released Enforcement Advisory No. 2024-01,[4] the California Privacy Protection Agency explains that a business subject to the CCPA *should* apply the principle of data minimization to every purpose for which it collects, uses, retains, and shares consumer personal information, but neither the advisory nor the CCPA *requires* data minimization to the degree mandated under MODPA.

- Blanket Prohibition on the Sale of Sensitive Data. The MODPA imposes strict limitations on the collection, processing, sharing and sale of sensitive data.[5] In line with the general data minimization requirement above, controllers cannot collect, process, or share sensitive data concerning a consumer except where such collection or processing is "*strictly necessary* to provide or maintain a specific product or service requested by the consumer to whom the personal data pertains."[6] (Emphasis added). This is a higher standard than "reasonably necessary and proportionate"—the general standard for the collection of personal data under the MODPA.

  Note that certain disclosures of personal data do not constitute a "sale" under MODPA.[7] These include (among other things): (i) disclosure of personal data to a third party for purposes of providing a product or service affirmatively requested by the consumer, (ii) disclosure or transfer of personal data to an affiliate of the

[4] Applying Data Minimization to Consumer Requests, California Privacy Protection Agency (Apr. 2024).

[5] "Sensitive data" means personal data that includes (1) data revealing: (i) racial or ethnic origin; (ii) religious beliefs; (iii) consumer health data, (iv) sex life, (v) sexual orientation, (vi) status as transgender or nonbinary; (vii) national origin; or (viii) citizenship or immigration status; (2) genetic data or biometric data; (3) personal data of a consumer that the controller knows or has reason to know is a child; or (4) precise geolocation data.

[6] Section 14-4607(A)(1).

[7] The MODPA defines a "sale of personal data" as "the exchange of personal data by a controller, a processor, or an affiliate of a controller or processor to a third party for monetary or other valuable consideration," subject to certain exceptions. (Section 14-4601(FF)).

controller, (iii) disclosure of personal data where the consumer (a) directs the controller to disclose the personal data or (b) intentionally uses the controller to interact with a third party.

- No Targeted Advertising to Minors Under 18. The MODPA is not unique in restricting the selling or sharing of children's personal data; the CCPA, for example, restricts such activities with respect to the personal information of minors under 16 years of age. However, the MODPA goes further in strictly prohibiting the sale, and the processing for targeted advertising, of personal data related to a consumer that "the controller knew or should have known… is under the age of 18 years."[8]

Implications for Businesses

For several years, state legislatures that were considering new comprehensive privacy laws had adhered to existing models—such as the CCPA or Virginia's Consumer Data Privacy Act[9]—to protect their residents without creating significant compliance burdens for businesses. With the MODPA, Maryland has thrown the proverbial monkey wrench into the mix. The unique elements of the MODPA—including strict data minimization, use limitations, and uniquely stringent restrictions on certain types of processing—are sufficiently different from other state privacy laws in that they may pose significant compliance challenges for national or regional businesses that operate, or target services to residents, in Maryland.

[8] The MODPA does not provide further information as to how to determine what a business "should have known."
[9] Va. Code §§ 59.1-575-59.1-585.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Laura E. Jehl
202 303 1056
ljehl@willkie.com

Susan Rohol
310 855 3172
srohol@willkie.com

Stefan Ducich
202 303 1168
sducich@willkie.com

Michelle Bae
202 303 1166
ebae@willkie.com