HINSHAW

Alerts

Maryland Legislature Passes Comprehensive Data Privacy Bill

April 19, 2024
Privacy, Cyber & AI Decoded

On April 6, 2024, Maryland's legislature passed a comprehensive privacy bill, the Maryland Online Data Privacy Act (MODPA), and sent it to the state's governor for signature. **If enacted, the law would take effect on October 1, 2025,** and become one of the strictest to date compared to other recently passed privacy laws.

What Makes Maryland's Bill Stricter than Other Privacy Laws?

For starters, it would apply more broadly and be easier to trigger, given the low applicability threshold. Indeed, it would cover persons who, "during the immediately preceding calendar year, controlled or processed the personal data of at least 35,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction" or "controlled or processed the personal data of at least 10,000 consumers and derived more than 90 percent of its gross revenue from the sale of personal data."

Employee data and HIPPA-covered data would be exempt, as would financial institutions subject to the Gramm-Leach-Bliley Act and those subject to the Fair Credit Reporting Act (FCRA) and any data covered by those laws. However, the law would still apply to nonprofits, institutions of higher education, and HIPPA-covered entities.

Key Maryland Online Data Privacy Act Provisions

1. Ban of Selling Sensitive Data

The bill would impose a complete ban on the sale of sensitive data, defined as an exchange of "monetary of other valuable consideration," which includes data related to an individual's race, religious beliefs, sex life or orientation, genetic or biometric data, consumer health data, or precise geolocation within 1,750 feet. However, although not listed as one, the definition of "sale" and "targeted advertising" suggests that consent continues to be a trump card.

The sale of personal data about individuals under the age of 18 would be banned, without exception, and unlike other state laws, would carry a "should have known" standard rather than, for example, one based on actual

Attorneys

Jason J. Oliveri

Service Areas

Privacy, Security & Artificial Intelligence

knowledge. Given the burden, it is anticipated that many covered entities may consider the use of age verification tools. Notably, on the same day the MODPA passed, the state also passed the Maryland Age-Appropriate Design Code Act. We will provide a separate article analyzing that bill once it is signed.

2. Increased Data Minimization Requirements

The heightened data minimization requirements are another feature where the bill deviates from those found in some of its sister states. Businesses would be limited to collecting personal data that is "reasonably necessary and proportionate to provide or maintain a product or service requested by the consumer to whom the data pertains."

The collection of sensitive data would be permissible if it is "strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the personal data pertains." Although the language of the bill suggests a difference between "reasonably necessary" and "strictly necessary," they are, unhelpfully, not defined. However, according to the International Association of Privacy Professionals (IAPP), a "should have known standard" can be interpreted as "…an affirmative duty to investigate who is visiting a website or app."

3. Data Protection Assessments

Data protection assessments are also required for processing activities that present a "heightened risk of harm" to consumers. Unlike other state laws, the MODPA imposes an obligation on covered entities to conduct an assessment "for each algorithm that is used." The assessment must identify and "weigh the benefits that may flow directly and indirectly from the processing to the controller, the consumer, other interested parties, and the public" against the potential risks.

Among other things, the consumer's reasonable expectations must be factored into the assessment. Covered entities should also be aware that the Maryland Consumer Protection Division (MCPD) may require the production of the assessment if it is relevant to an investigation they are conducting. Although, they should also note that one is only required for activities occurring after October 1, 2025.

4. Unique Targeted Advertising Requirements

The bill also features unique requirements for targeted advertising. Like other states, it gives consumers the right to opt out of such processing but prohibits the processing of personal data for targeted advertising if the controller knew or should have known that the individual was under the age of 18.

However, if consent has been obtained or the processing is necessary for the provision of goods and services. Notably, most states only require opt-in consent when the consumer is either 13 or 16 years old or younger.

5. Opt-out Rights and Updated Privacy Notices

The bill also has familiar features that covered entities will recognize, such as the requirement that they post an up-to-date and "reasonably accessible, clear, and meaningful privacy notice." The requirements concerning data processing agreements also likely will not cause much of a stir. Additionally, the bill provides some leniency not found in other laws in connection with universal opt-out mechanisms, which are optional.

Covered entities can provide a link on their website for consumers to exercise their opt-out rights or enable the use of an opt-out preference signal – a departure from those states that require both.

For those not in complete compliance by the effective date, the Attorney General may provide a 60-day notice and cure period before the commencement of any action, which sunsets April 1, 2027. Violations may result in fees of up to $10,000 per violation, and if the fee is for a repeated violation, the fees may climb to $25,000 per violation.

What's Next?

In sum, Maryland is considering a privacy law that, in some ways, resembles those found in sister states but, in other respects, appears to take things a step further, much to the delight of many privacy advocates. It is anticipated that the law will be enacted and that it will raise a number of compliance questions. As such, it may behoove covered businesses to start considering their new compliance goals sooner rather than later.

Law clerk Sabrina Messar contributed to this post. She is not currently admitted to practice law.