PUBLICATION

Practical Next Steps for Businesses as Maryland's Updated Consumer Data Privacy Laws Take Effect in October

Authors: Alexandra P. Moylan, Michael J. Halaiko, Dandridge S. Parks

September 03, 2025

Maryland's Online Data Privacy Act of 2024 (MODPA) will take effect on October 1, 2025, and will be enforced by the Maryland Attorney General (AG) beginning April 1, 2026. MODPA sets a new, more stringent benchmark among U.S. state privacy laws. Businesses that process the personal data of Maryland residents should begin preparing now.

MODPA's Broad Applicability and Limited Exemptions Are Unique

MODPA applies to entities that conduct business in Maryland or provide products or services targeted to Maryland residents, and during the immediately preceding calendar year either:

- 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 20 percent of its gross revenue from the sale of personal data.

Entities exempt from the law's requirements are limited and include governmental bodies and financial institutions or affiliates subject to Title V of the Gramm-Leach-Bliley Act, among others. Unlike other state consumer privacy laws, MODPA does not have entity-level exemptions for nonprofit organizations, HIPAA-covered entities, higher education institutions, or small businesses. Nonprofit organizations that process personal data solely for the purpose of assisting (i) law enforcement in investigating criminal or fraudulent acts relating to insurance or (ii) first responders in responding to catastrophic events are exempt. Similarly, there are data-level exemptions for personal data regulated by HIPAA (i.e., protected health information), personal data subject to regulation under FERPA, and personal data processed by consumer credit reporting agencies subject to the Fair Credit Reporting Act, among others.

MODPA's thresholds for applicability are low compared to other state privacy laws. When coupled with the relatively short list of entity-level exemptions, entities that do business in Maryland will need to examine potential applicability of the law, even if traditionally exempt under other state privacy laws.

Why MODPA Is Among One of the Strictest U.S. State Consumer Privacy Laws

Data Minimization Mandate

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. This strict data minimization standard applies even if the consumer provides consent. The statute, however, does not define "reasonably necessary and proportionate." The AG has not issued any guidance on MODPA.

Broad Definition of "Sensitive Data"

"Sensitive data" includes, among other categories: biometric data; genetic data; precise geolocation data (within a radius of 1,750 feet); consumer health data; data about a consumer known to be a child; and information revealing sexual orientation, gender identity, racial or ethnic origin, religious beliefs, citizenship, or immigration status. The sale of any sensitive data is categorically prohibited, regardless of consent. Controllers may not collect, process, or share sensitive data unless it is **strictly necessary** to provide or maintain a specific product or service requested by the consumer, or the controller has obtained the consumer's consent. Like the data minimization standard, the "strictly necessary" standard is not defined.

Protection of Children and Teenagers (Ages 13 - 17)

- **Targeted Advertising**: A controller may not process personal data for targeted advertising if the controller knows or should know that the consumer is under the age of 18.
- **Sale of Personal Data**: The sale of personal data of a consumer under the age of 18 is prohibited.

Children under 13 remain subject to the Children's Online Privacy Protection Act (COPPA) and parental-consent requirements.

Along with MODPA, Maryland passed the Maryland Kids Code, which regulates businesses that offer online products reasonably likely to be accessed by children under age 18 and has been in effect since October 1, 2024.

Universal Opt-Out Signal Requirements

By October 1, 2025, controllers must enable consumers to opt out of targeted advertising and the sale of personal data via an opt-out preference signal (such as a browser or device-level signal). Controllers must also provide a clear and conspicuous web-link opt-out mechanism.

Geofencing Ban for Health Data

It is unlawful to use a geofence within 1,750 feet of a mental health facility or a reproductive or sexual health facility for the purpose of identifying, tracking, collecting data from, or sending notifications to a consumer.

Consumer Rights

Consumers may exercise the familiar bundle of rights: access, correction, deletion, portability, and opt-out of (i) targeted advertising, (ii) sale of personal data, and (iii) certain profiling. Controllers must respond within 45 days (extendable once by 45 days) and provide an appeal mechanism. One request per 12-month period must be fulfilled free of charge.

Governance Obligations

Privacy Notice

Controllers must provide a "reasonably accessible, clear, and meaningful" privacy notice that discloses, among other items, all categories of personal and sensitive data processed and shared, processing purposes, third-party categories, and instructions for exercising rights.

Opt-Out Infrastructure

Controllers must (i) offer a conspicuous web-link opt-out or (ii) on or before October 1, 2025, honor a universal opt-out signal.

Contracts with Processors

A written contract is required and must, at a minimum, set out processing instructions, confidentiality obligations, security measures, audit rights, and subcontractor flow-down requirements.

Data Protection Assessments (DPAs)

Controllers must conduct and document a Data Protection Assessment (DPA) for each processing activity that presents a "heightened risk of harm" to a consumer, including:

processing personal data for targeted advertising;

sale of personal data;

processing of sensitive data;

processing data for profiling if there's a risk of unfair, abusive, or deceptive treatment or if it will have an unlawful disparate impact, financial, physical, reputational, or other substantial injury to a consumer; and

processing that intrudes on the solitude or seclusion of the private affairs of a consumer.

DPAs are required only for processing activities that occur on or after October 1, 2025, and must be made available to the AG upon request but otherwise remain confidential and exempt from disclosure.

Security Requirements

Controllers and processors must implement "reasonable administrative, technical, and physical" measures to protect the confidentiality, integrity, and accessibility of the personal data they process commensurate with the volume and personal data that they process.

Enforcement

Violations constitute an "unfair, abusive, or deceptive trade practice" under the Maryland Consumer Protection Act (MCPA), subject to civil penalties of up to $10,000 per violation for a first offense and $25,000 per violation for repeat offenses, plus injunctive relief. Given the number of individuals whose data many companies handle, those fines can quickly multiply, and the potential exposure is significant. However, there is no private right of action under MODPA.

For alleged violations occurring on or before April 1, 2027, the AG may issue a notice of violation and allow at least 60 days to cure if the AG determines a cure is possible, considering factors such as the number of violations and likelihood of injury. After April 1, 2027, the AG may proceed directly to enforcement without a cure period.

Practical Next Steps for Businesses

1. **Scope Analysis:** Confirm whether your organization meets MODPA's volume/revenue thresholds.
2. **Data Mapping and Classification:** Identify whether your organization is processing sensitive data, processing personal data for the purposes of profiling, processing personal data for the purposes of targeted ads, selling personal data, or processing children's data, and implement a policy for MODPA compliance.
3. **Revise Collection Practices:** Align data flows with the "reasonably necessary and proportionate" minimization standard.
4. **Update Privacy Disclosures:** Reflect all MODPA-required content and remove blanket consents that may no longer suffice.

5. **Build Opt-Out Infrastructure:** Implement mechanisms to recognize universal opt-out signals and honor minor-consent requirements.
6. **Conduct DPAs:** Prioritize high-risk processing and algorithmic uses; document DPAs before go-live.
7. **Assess AI usage:** MODPA's stricter data minimization requirements and sensitive data restrictions (as well as DPA requirements for algorithms) could impact usage and development of AI.
8. **Contract Management:** Insert MODPA-compliant clauses in all processor, vendor, and AdTech agreements.
9. **Incident Response and Geofencing Review:** Ensure there is no geofencing around protected health-care locations and update incident-response playbooks.
10. **Training and Governance:** Educate product, engineering, marketing, and customer-service teams on MODPA requirements and response timelines.
11. **Monitor Rulemaking:** While the statute is self-executing, the AG may issue guidance; maintain a horizon-scanning process.

Conclusion

MODPA's stringent data-minimization mandate, outright ban on selling sensitive data, enhanced protections for teens, and early-adopter requirement to honor universal opt-out signals collectively raise the U.S. privacy bar. Organizations that act now – by tightening data-collection practices, refreshing privacy notices, executing DPAs, and operationalizing new opt-out workflows – will be best positioned to comply when enforcement begins in April 2026.

For assistance in assessing your organization's strategic data goals and compliance readiness under MODPA or other U.S. state privacy laws, please contact the authors or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.