MARYLAND ONLINE DATA PRIVACY ACT (MODPA)

CHECKLIST

USERCENTRICS

Maryland Online Data Privacy Act (MODPA) gives Maryland residents rights over how their personal data is collected and used.

This checklist walks through steps that support your compliance efforts under the Act, along with recommended best practices for privacy-related user experience.

Important to know:

Action	Date
Effective date	October 1, 2025
Enforceable against processing activities	Since April 1, 2026
Retroactive	No
2026 amendment (HB 711)	Expanded "sensitive data" to include inferred sensitive data; restricted sale of personal data to government entities recently engaged in or supporting immigration enforcement
Cure period	60 days, discretionary, sunsets April 1, 2027

1 Determine If Your Company Is Required to Comply

If your for-profit organization:

- Controls or processes personal data of at least 35,000 Maryland consumers annually, excluding data processed solely to complete a payment transaction, or
- Controls or processes personal data of at least 10,000 consumers, and derives more than 20 percent of gross revenue from the sale of personal data

There is no minimum annual revenue floor.

Entity-level exemptions:

- State agencies or political subdivisions
- National securities associations under the Federal Securities Exchange Act, or registered futures associations under the Federal Commodity Exchange Act
- GLBA-regulated financial institutions or affiliates
- Nonprofit controllers that process or share personal data solely to assist law enforcement investigating insurance-related crime or fraud, or to assist first responders responding to catastrophic events

Data-level exemptions:

- Protected healthcare-related information
- Patient-identifying information
- Research data
- Data created for or collected under several federal laws, including, among others:
  - HIPAA
  - FCRA
  - Driver's Privacy Protection Act
  - FERPA
  - Farm Credit Act
  - Airline Deregulation Act

2 Create a Comprehensive Privacy Policy

Businesses are required to inform consumers at or before the point of data collection about:

- Categories of personal data processed
- Purposes for which data is processed
- Categories of personal data the controller shares with third parties, if any
- Categories of third parties the controller shares personal data with, if any

Rights: Inform website visitors of their privacy rights and how to exercise them, including how a consumer may appeal a controller's decision.

Language: Keep the privacy policy clear and easy to understand.

Implementation: As a best practice, pair the privacy notice with an opt-out mechanism. For example, use a Privacy Policy Generator and a CMP to manage opt-outs.

3 Apply Maryland's Stricter Data Minimization Standard

Collect only personal data that is reasonably necessary and proportionate to provide the product or service the consumer requested. This standard is stricter than most peer state laws.

4 Honor Universal Opt-Out Signals

Recognize a consumer's opt-out preference signal (e.g., Global Privacy Control) as a valid method of opting out of the sale of personal data, targeted advertising, and profiling. There is no exemption from this requirement.

5 Restrict Sensitive Data Under the 2026 Amendment

Do not sell sensitive personal data under any circumstances. This includes data now classified as sensitive because it is inferred from other personal data (per HB 711, 2026). Do not sell personal data to any government entity that, within the preceding six months, has engaged in or supported immigration enforcement.

6 Enable Clear Options When Consent Is Required

When: If the personal data collected is sensitive, or that of a child.

Availability: Easily accessible on your website.

Method: Via a CMP.

7 Authenticate Consent for Collection of Sensitive Personal Data or Data From Minors

Sensitive personal data: Affirmative opt-in consent is required for processing sensitive personal data.

Consent for children: Obtain consent from a parent or legal guardian for collection of personal data if the data subject is 13 or younger.

8 Inform Consumers About Their Rights

Consumers' rights under the MODPA:

- **Right to access:** Request and receive a copy of their personal data
- **Right to correction:** Updates or corrections to inaccuracies in personal data collected
- **Right to deletion:** Personal data that has been collected about them (with exceptions)

- **Right to data portability:** Copy of personal data must be provided in a portable and readily useable format
- **Right to opt out:** Of processing of personal data for the purposes of sale, targeted advertising, or profiling
- **Right to nondiscrimination:** For exercising privacy rights
- **Right of minors:** Consent must be obtained from a parent or guardian before children's (under age 13) personal data is collected

9 As a Best Practice, Review and Update Your Privacy Policy Every 12 Months

Review your operations and any changes in the law every 12 months. Update the privacy policy and its effective date, even if no other changes are made.

Transparency: Keep the information visitors must be notified about clear, comprehensive, and up to date, with the last-update date clearly visible.

Data sold: List all categories of personal information your business has sold in the past 12 months.

10 Enable Consumers to Make Data Subject Access Requests (DSARs)

Provide one or more contact options (e.g., toll-free phone number, web form, email). Set up a system to enable submission of DSARs.

11 Set Up a System to Verify Data Subject Access Requests (DSARs)

As a best practice, enable consumers to attach documentation to help verify their identity and residency. If your business cannot reasonably verify a consumer's identity, inform them and explain why, and enable them to rectify.

12 Keep Track of Data Subject Access Requests (DSARs)

Set up a system to track all requests. Keep records of requests and responses for 2 years after the last consumer interaction.

13 Fulfill Data Subject Access Requests (DSARs)

Respond to DSARs within 45 days, extendable by a further 45 days with notice to the consumer.

Falling thresholds, rising enforcement and litigation, eroding ad revenue. Do you know your risk?

GET IN TOUCH