Now & Next
Healthcare & Data Privacy Alert

May 20, 2024

Maryland enacts comprehensive data privacy act

By Meredith LaMaster and Julia Cassidy

The *Maryland Online Data Privacy Act of 2024* (MODPA) requires stricter protections for sensitive data and offers opt-outs from targeted advertisements and the sale of personal data.

What's the impact?

- MODPA outlines consumer rights, obligations for individuals and entities using data, and factors determining if and when enforcement may commence.
- Businesses serving Maryland residents will need to evaluate their privacy practices to make necessary adjustments to comply with MODPA's consumer request and opt-out requirements.

On May 9, 2024, Maryland became the fifth state to enact a data privacy law in 2024 and the seventeenth state overall. Unlike other state privacy laws with a similar substantive framework, MODPA imposes more rigorous restrictions on data controllers (Controllers) and processors (Processors) and offers consumers more protections with regard to their personal data. MODPA goes into effect on October 1, 2025, but will not affect any personal data processing activities until April 1, 2026.

Definitions under MODPA

CONTROLLER

A person who, alone or jointly with others, determines the purpose and means of processing personal data.

PERSONAL DATA

Any information that is linked or can be reasonably linked to an identified or identifiable consumer. "Personal data" **does not include** (i) de-identified data or (ii) publicly available information.

PROCESS

An operation or set of operations performed by manual or automated means on personal data. "Process" includes collecting, using, storing, disclosing, analyzing, deleting, or modifying personal data.

PROCESSOR

A person who processes personal data on behalf of a Controller.

SENSITIVE DATA

Personal data that includes the following:

- Data revealing:
  - Racial or ethnic origin
  - Religious beliefs
  - Consumer health data
  - Sex life
  - Sexual orientation
  - Status as transgender or nonbinary
  - National origin
  - Citizenship or immigration status
- Genetic data or biometric data
- Personal data of a consumer the Controller knows or has reason to know is a child
- Precise geolocation data.

MODPA applicability

MODPA applies to a person, whether that be an individual or in conjunction with others, who conducts business in Maryland or provides products or services directed toward Maryland residents during the prior calendar year either:

- Controlled or processed the personal data of 35,000 or more consumers, with the exception of personal data controlled or processed solely to effectuate payment or
- Controlled or processed the personal data of 10,000 or more consumers, in addition to obtaining at least twenty percent (20%) of gross revenue from personal data sales.

Twenty percent (20%) is a lower revenue threshold than seen in many other states, which increases the number of businesses likely subject to MODPA's requirements.

MODPA exemptions

While MODPA covers a wide swath of entities, several categories are exempt, including:

- Regulatory, administrative, advisory, executive, appointive, legislative, or judicial bodies of Maryland
- Registered national securities and futures associations
- Financial institutions and their affiliates subject to the Gramm-Leach-Bliley Act
- Nonprofit Controllers that process or share data solely to assist law enforcement agencies investigating insurance fraud or first responders responding to catastrophic events

In addition to exempt entities, MODPA does not regulate certain data and information, including protected health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), identifiable private information related to protecting human subjects, de-identified data, medical records held by covered entities or business associates, data used and maintained for emergency contact situations, or data covered under the federal Fair Credit Reporting Act (FCRA), Driver's Privacy Protection Act of 1994, Family Educational Rights and Privacy Act (FERPA), Farm Credit Act, and Airline Deregulation Act.

Consumer rights under MODPA

Under MODPA, consumers are granted certain rights with respect to personal data, including the right to:

- Inquire as to whether a Controller is processing the consumer's personal data.
- Access personal data if a Controller is processing it.
- Depending upon the nature and purposes for processing the personal data, correct inaccuracies of the personal data.

- Mandate that the Controller delete personal data provided by or attained about the consumer unless retention is required by law.
- If processing is done automatically, obtain a copy of the processed personal data in an easily readable format.
- Receive a categorized list of third parties that the Controller has disclosed the consumer's personal data to.
- Opt out of:
  - Targeted advertisements,
  - Personal data sales, and
  - Profiling.

Obligations for data controllers and processors

MODPA establishes several obligations and restrictions upon subject entities.

CONTROLLER RESTRICTIONS

Controllers may not:

- Collect, process, or share personal data, except when strictly necessary to provide or maintain a specific product or service requested by the consumer and after having obtained the consumer's consent.
- Sell sensitive data.
- Process personal data that violates laws prohibiting unlawful discrimination.
- Process personal data for targeted advertisements if the Controller knew or should have known that the data belonged to someone under eighteen (18) years of age.
- Sell a consumer's data if the Controller knew or should have known that the consumer is under eighteen (18) years of age.
- Discriminate against a consumer for exercising their rights under MODPA, including denying goods or services, charging different prices, or providing lower quality services or goods to the consumer.
- Collect, process, or transfer personal or publicly available data that could be used to discriminate against and disrupt a consumer's equal enjoyment of goods and services unless (i) the Controller is self-testing to prevent or mitigate unlawful discrimination, (ii) the Controller is using the data to diversify an applicant, participant, or customer pool, or (iii) the Controller is a private club or group.
- Unless consumer consent is obtained, process personal data for purposes that are not reasonably necessary nor in alignment with the disclosed purposes for which the data is

processed.

- Provide an employee or contractor access to consumer health data unless:
  - The employee or contractor is contractually or statutorily bound by a confidentiality obligation or
  - Confidentiality is required as a condition of employment.
- Provide a Processor access to consumer health data unless a contract is in place.
- Use a geofence to establish a virtual boundary within 1,750 feet of a mental health facility or reproductive or sexual health facility to identify, track, or collect data or send a consumer a notification regarding their health data.

CONTROLLER REQUIREMENTS

Controllers are required to:

- Limit personal data collection to what is reasonably necessary and proportionate to providing or maintaining a specific product or service requested by the consumer.
- Establish, implement, and maintain appropriate administrative, technical, and physical data security safeguards to protect the confidentiality, integrity, and accessibility of personal data.
- Provide an effective mechanism for consumers to revoke consent that is at least as easy as the mechanism used by the consumer to provide consent.

When a consumer revokes consent, the Controller must stop processing personal data as soon as possible but no later than thirty (30) days after receiving the request.

PRIVACY NOTICES

Controllers must provide consumers with a clear privacy notice that includes the following:

- Categories of personal data processed by the Controller, including sensitive data;
- Why the Controller is processing personal data;
- How consumers may exercise their rights under MODPA, including the right to appeal or revoke consent;
- The categories of third parties that the Controller shares personal data with and details on the type of, business model of, or processing conducted by each third party;
- Categories of personal data, including sensitive data, shared with third parties; and
- An active email address or other online option through which the consumer can contact the Controller.

DISCLOSURE REQUIREMENT

If a Controller sells personal data to third parties or processes personal data for targeted advertisements or to profile customers, the Controller must clearly and conspicuously disclose the sale or processing, in addition to how a consumer can opt out.

COMPLYING WITH MODPA REQUIREMENTS

Controllers may:

- Provide a clear and conspicuous link on the Controller's website that allows a consumer, or their authorized agent, to opt out of the targeted advertisements or the sale of the consumer's data or
- On October 1, 2025, allow the consumer to opt out of targeted advertisements or the sale of the consumer's data.

CONTRACTING WITH PROCESSORS

When a Controller uses a Processor to process consumers' personal data, the two entities must enter into a written contract outlining the Processor's data processing procedures as they relate to the services that will be performed on behalf of the Controller. The contract must specify the following:

- Instructions for processing data
- Nature and purpose of processing
- Type of data subject to processing
- Duration of processing
- Both parties' rights and obligations

DATA PROTECTION ASSESSMENTS

Controllers must regularly conduct and document data protection assessments for all data processing activities that present an elevated risk of harm to a consumer, including an assessment for each algorithm. The data protection assessment must identify and weigh direct and indirect benefits to the Controller, the consumer, other interested parties, and the public against the following:

- Potential risks to consumer rights associated with processing as mitigated by Controller-employed safeguards to reduce risks and
- The necessity and proportionality of processing as they relate to the stated purpose of the processing.

Upon request, Processors must provide properly conducted assessment reports to a Controller. Controllers that utilize Processors must provide clear instructions on how to process personal data.

Enforcement authority

Before handing down an enforcement action, the Maryland Office of the Attorney General, Consumer Protection Division (the Division), which has exclusive enforcement authority, can issue a notice of violation to a Controller or Processor if a cure is deemed possible. Upon receipt of the notice of violation, the Controller or Processor has at least sixty (60) days to cure the violation. If the Controller or Processor fails to do so within the prescribed time period, the Division may then bring an enforcement action. When deciding whether to grant a Controller or Processor the opportunity to cure an alleged violation, the following factors may be considered:

- Number of violations
- Controller or Processor's size and complexity
- Nature and breadth of the Controller or Processor's processing activities
- Possibility of injury to the public
- Security of persons or property
- Likelihood the alleged violation was caused by human or technical error
- Controller or Processor's history of violations

Businesses must prioritize data privacy compliance

As data privacy continues to play a prominent role in the news, more states are expected to promulgate comprehensive acts to protect their residents. As a result, businesses offering goods and services to residents of states with data privacy acts will need to evaluate their business and privacy practices on an ongoing basis to ensure they align with state requirements.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Meredith D. LaMaster
312.977.9257
mlamaster@nixonpeabody.com

Julia E. Cassidy
212.940.3137
jcassidy@nixonpeabody.com