Department of Legislative Services

Maryland General Assembly
2024 Session

FISCAL AND POLICY NOTE
Enrolled - Revised

Senate Bill 541 (Senator Gile, *et al.*)
Finance Economic Matters

Maryland Online Data Privacy Act of 2024

This bill establishes numerous consumer protections and regulatory requirements related to online data. Certain requirements and obligations for a "controller" or "processor" apply only prospectively and may not be applied or interpreted to have any effect on (or application to) any personal data processing activities before April 1, 2026. Violation of the bill is an unfair, abusive, or deceptive trade practice under the Maryland Consumer Protection Act (MCPA), subject to MCPA's civil and criminal penalty provisions. However, a violator is not subject to specified MCPA penalty provisions related to private causes of actions for damages. The bill contains a severability clause. **The bill takes effect October 1, 2025.**

Fiscal Summary

State Effect: General fund expenditures likely increase, at least minimally, for the Office of the Attorney General (OAG), Consumer Protection Division beginning in FY 2026, as discussed below. The bill's imposition of existing penalty provisions is not anticipated to have a material impact on State revenues.

Local Effect: The bill's imposition of existing penalty provisions does not have a material impact on local government finances or operations.

Small Business Effect: Meaningful.

Analysis

Bill Summary:

Definitions and Applicability

The bill defines several terms related to online and biometric data privacy. Notably, a "controller" is person that determines the purpose and means of processing personal data – either alone or jointly with others. A "processor" is a person that processes personal data on behalf of a controller.

The bill specifies the types of data and entities to which its requirements apply. Specifically, the bill applies to a person that conducts business in the State or provides products or services that are targeted to residents of the State, and that during the preceding calendar year did any of the following:

- 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% of its gross revenue from the sale of personal data.

The bill specifies several entities to which its requirements do not apply, including State and local agencies, courts, and certain types of businesses subject to related federal laws. Additionally, certain data is also exempt from the bill's requirements, including specified health and financial data.

Consumer Rights and Controller Responsibilities

The bill defines the rights a consumer may exercise to protect the consumer's personal data, including, among other things, the right to require the deletion of personal data provided by (or obtained about) the consumer (unless retention of the personal data is required by law) and to opt out of the processing of personal data (*e.g.*, targeted advertising).

The bill establishes a number of consumer protections, including:

- requiring a controller of data to establish a secure and reliable method for a consumer to exercise a right;
- establishing a timeframe and related requirements for a controller to respond to and/or comply with a request from a consumer;

- requiring the controller to notify the consumer in a specified manner if the controller chooses not to take action on a request;
- requiring a controller to provide a consumer, free of charge, with the information a consumer requests, subject to certain limitations; and
- requiring a controller to establish a process that a consumer may use to appeal a controller decision.

Limitations

The bill specifies limitations on the requirements established for controllers and processors. Among other things, the bill may not be construed to prohibit a controller or processor from (1) complying with federal, State, or local laws or authorities; (2) preserving the integrity or security of a system; or (3) assisting another controller, processor, or third party with an obligation under the bill.

Additionally, the bill's requirements may not restrict a controller's or processor's ability to collect, use, or retain data for internal use to effectuate a product recall, identify and repair technical errors, or perform internal operations, as specified.

Designation of Authorized Agent

A consumer may designate an authorized agent to act on the consumer's behalf to opt out of the consumer's personal data processing, as specified, and certain individuals, such as the parent or legal guardian of a known child, may exercise the consumer rights directly on behalf of another individual.

Other Rules, Procedures, and Prohibitions

The bill establishes numerous rules, procedures, and prohibitions related to controllers and processors. For instance, the bill:

- requires a controller to 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;
- requires a controller to provide an effective mechanism for a consumer to revoke the consumer's consent and to stop processing the data no later than 30 days after the receipt of the request;
- prohibits discrimination against any consumer for exercising a right granted by the bill, as specified;
- requires a controller to disclose specified information when it sells personal data to third parties or processes personal data for targeted advertising;

- requires a controller to provide a consumer with a reasonably accessible, clear, and meaningful privacy notice that includes specified information about the controller's data processing practices and information about how a consumer can exercise a right granted by the bill;
- requires a controller and processor to enter into a contract that includes specified requirements if a controller uses a processor to process the personal data of consumers;
- defines the responsibilities of both the controller and processor in the event that such a contract is entered into; and
- establishes more stringent procedures and requirements for processing activities that present heightened risk of harm to a consumer (*e.g.*, the processing of sensitive data).

The bill authorizes OAG to require a controller to make available a data protection assessment for compliance with the responsibilities established by the bill. The assessment is confidential and exempt from disclosure requirements under the Maryland Public Information Act. A data protection assessment conducted under these provisions must apply to processing activities that occur on or after October 1, 2025, and is not required for processing activities that occur prior to that date.

The bill establishes procedures and requirements related to enforcement actions by OAG. Specifically, before initiating an enforcement action pursuant to the bill, OAG may issue a notice of violation to the controller or the processor if OAG determines a cure is possible. If such a notice is issued, the controller or processor must have at least 60 days to cure the violation after receipt of the notice. However, if the violation is not cured within the required time period (specified by OAG), then OAG may bring an enforcement action pursuant to the bill's authorization. In determining whether to grant a controller or processor an opportunity to cure an alleged violation, OAG may consider specified factors (*e.g.*, the number of violations, the size and complexity of the controller or processor, the likelihood of injury to the public, etc.). These provisions are applicable to enforcement actions for alleged violations that occur on or before April 1, 2027.

Current Law: The Maryland Personal Information Protection Act (MPIPA) defines "personal information" as, among other things, biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account in combination with an individual's first name or first initial and last name, when the name or data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable.

MPIPA imposes certain duties on a business to protect an individual's personal information. A business in possession of personal information must implement and maintain reasonable security procedures and practices to protect the information from unauthorized access, use, modification, or disclosure. If a data breach occurs, the business must conduct, in good faith, a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been (or will be) misused. If the business determines that personal information likely has been (or will be) misused, the owner or licensee of the computerized data must notify an affected individual as soon as practicable but not later than 45 days after the business discovers or is notified of the breach. For a business that only maintains personal data, the business must notify the owner or licensee of the breach as soon as practicable but not later than 10 days after the business discovers or is notified of the breach. Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security.

When a breach occurs, a business must also provide notice to OAG that includes (1) the number of Maryland residents affected by the breach; (2) a description of the breach, including when and how the breach occurred; (3) any steps the business has taken or plans to take relating to the breach; and (4) the form of notice and a sample of the notice that will be sent to individuals affected by the breach. The Act also establishes a specific notification process for breaches involving email account information.

Violation of MPIPA is an unfair, abusive, or deceptive trade practice under MCPA, subject to MCPA's civil and criminal penalty provisions.

Maryland Consumer Protection Act

An unfair, abusive, or deceptive trade practice under MCPA includes, among other acts, any false, falsely disparaging, or misleading oral or written statement, visual description, or other representation of any kind, which has the capacity, tendency, or effect of deceiving or misleading consumers. The prohibition against engaging in any unfair, abusive, or deceptive trade practice encompasses the offer for or actual sale, lease, rental, loan, or bailment of any consumer goods, consumer realty, or consumer services; the extension of consumer credit; the collection of consumer debt; or the offer for or actual purchase of consumer goods or consumer realty from a consumer by a merchant whose business includes paying off consumer debt in connection with the purchase of any consumer goods or consumer realty from a consumer.

The Consumer Protection Division is responsible for enforcing MCPA and investigating the complaints of aggrieved consumers. The division may attempt to conciliate the matter, issue a cease and desist order, or file a civil action in court. A merchant who violates MCPA is subject to a fine of up to $10,000 for each violation and up to $25,000 for each repetition

of the same violation. In addition to any civil penalties that may be imposed, any person who violates MCPA is guilty of a misdemeanor and, on conviction, is subject to a fine of up to $1,000 and/or imprisonment for up to one year.

State Expenditures: General fund expenditures likely increase, at least minimally, for OAG to handle enforcement under the bill. OAG advises that it may require as many as four additional positions (one full-time assistant Attorney General, two investigators, and one mediator) with corresponding general fund expenditures of up to $390,900 in fiscal 2026, accounting for the bill's October 1, 2025 effective date, and $539,200 by fiscal 2030.

However, the Department of Legislative Services advises that the extent of resources potentially needed by OAG is dependent on the number of complaints filed under the bill and the level of effort involved in each case. While generally acknowledging that expenditures likely increase at least minimally for enforcement efforts, without experience under the bill, the need for additional staff is unclear. To the extent that additional staffing resources are required, OAG may request them through the annual budget process.

Small Business Effect: The bill establishes a significant regulatory framework related to online and biometric data. Thus, to the extent any small businesses in the State qualify as a controller and/or processor, they may be meaningfully affected.

Additional Information

Recent Prior Introductions: Similar legislation has been introduced within the last three years. See HB 807 of 2023.

Designated Cross File: HB 567 (Delegate Love, *et al.*) - Economic Matters.

Information Source(s): Prince George's County; Office of the Attorney General (Consumer Protection Division); Judiciary (Administrative Office of the Courts); Department of State Police; Maryland Department of Transportation; Department of Legislative Services

Fiscal Note History: First Reader - February 12, 2024
rh/jkb Third Reader - March 27, 2024
Revised - Amendment(s) - March 27, 2024
Enrolled - May 2, 2024
Revised - Amendment(s) - May 2, 2024

Analysis by: Eric F. Pierce

Direct Inquiries to:
(410) 946-5510
(301) 970-5510