Department of Legislative Services

Maryland General Assembly
2026 Session

FISCAL AND POLICY NOTE
First Reader

House Bill 264 (Chair, Government, Labor, and Elections Committee)(By Request - Departmental - Information Technology)

Government, Labor, and Elections

Maryland Data Privacy and Protection Act of 2026

This departmental bill limits the personal information that may be collected, maintained, processed, and retained by units of State government and requires certain personal information to be deleted or de-identified. Each unit of State government must post a privacy notice on its website, as specified, and designate a Privacy Officer. The Department of Information Technology (DoIT) is required to establish additional security requirements in applicable contracts. The bill also expands the definition of "personal information" as it relates to the protection of information by government agencies.

Fiscal Summary

State Effect: Although the bill can generally be implemented within the existing resources of most State agencies, others may incur additional costs (primarily for staff) to meet the bill's requirements, as discussed below. Revenues are not affected.

Local Effect: The bill is not anticipated to materially affect local government operations or finances.

Small Business Effect: DoIT has determined that this bill has minimal or no impact on small business (attached). The Department of Legislative Services concurs with this assessment.

Analysis

Bill Summary:

Public Information Act – Personal Records

Specific to the Public Information Act, the bill requires personal information collected by units of the State (*i.e.*, State and local government entities) for personal records to be:

- appropriate and relevant to the *legitimate government purpose* for which it is collected;
- limited to the minimum amount of personal information necessary to accomplish the legitimate government purpose for which it was collected;
- retained for only as long as is reasonably necessary to fulfill the legitimate government purpose for which it was collected; and
- securely deleted or de-identified when no longer needed to fulfill the legitimate government purpose for which it was collected.

Similarly, an official custodian who requests personal information for personal records must provide the *legitimate government* purpose for which the personal information is collected.

Each unit of the State must post a privacy notice (in addition to its privacy policies, which are required to be posted under current law). The privacy notice and privacy policies must be consistent with the guidelines, standards, and policies that the bill requires DoIT to adopt.

The bill exempts information contained in application or renewal materials relating to the licensing, registration, or certification of an individual for an occupation or profession from the requirements noted above.

Compliance with Information Processing and Security Requirements

The bill requires each unit of State government (*i.e.*, State agencies) to designate a Privacy Officer to oversee compliance with information processing and security requirements required by State law. The Privacy Officer must also coordinate with DoIT and the Office of the Attorney General (OAG). Additionally, DoIT must adopt regulations, guidance, and model templates to support compliance, including standard Public Information Act formats and data protection protocols.

Procurement Contracts – Basic Security Requirements

The bill expands provisions specifying that DoIT must require basic security requirements in a contract; under the bill, it must also require *data collection and privacy* requirements in a contract under which a third-party contractor will (1) have access to and use State *information technology* equipment, systems, or services; (2) collect, store, or process personal information as defined in § 10-1301 of the State Government Article (as amended by the bill); or (3) connect to State *information technology* equipment, systems, or services.

The privacy requirements noted above must be consistent with widely recognized privacy standards, including specified standards developed by the National Institute of Standards and Technology.

Protection of Information by Government Agencies

The bill expands the definition of "personal information" within provisions of State law governing the protection of information by government entities (which includes State and local agencies). Specifically, the bill adds the following data elements that constitute "personal information" *when combined* with an individual's first name (or first initial) and last name, personal mark, or unique biometric or genetic print or image:

- a username or e-mail address in combination with a password or security question and answer that permits access to an individual's e-mail account;
- genetic and health-related data, including mental health, substance use disorder, and disability; or
- sensitive data, which generally means personal data that reveals certain demographic, genetic, biometric, or education information about an individual.

Current Law:

State Chief Privacy Officer and Agency Privacy Officers

Executive Order 01.01.2021.10 was signed in 2021 and established the State Chief Privacy Officer (SCPO) in the Office of the Governor to, among other things, provide the Governor with advice, recommendations, and consultation about data privacy; supervise and direct efforts of State units to protect and secure personally identifiable information (PII), and assist State units with various duties related to the collection, processing, sharing, and protection of PII.

The Executive Order also requires many, but not all, State agencies to, among other duties, employ reasonable security practices and procedures, designate an agency privacy official, comply with direction from the SCPO, as specified, adopt a privacy governance and risk

management program, and allow an individual to opt out of the State unit's sharing of information if the sharing is not required by law. Agency privacy officers must meet at least monthly to provide the SCPO with advice and recommendations about State polices needed to protect the privacy of PII. Agencies specified by the Executive Order must, by April 1 each year, submit a report to the SCPO that includes:

- an inventory of all information systems and applications used or maintained by the State unit;
- a full data inventory of the State unit;
- a list of all cloud services used by the State unit; and
- a list of all permanent and transient vendor interconnections that are in place.

Data Protection by State Agencies and Local Governments

Generally, a unit of State or local government (except for the Legislative and Judicial branches of State government) that collects an individual's personal information must implement and maintain reasonable security procedures and practices appropriate to the nature of the information collected and the nature of the unit and its operations. Similarly, a unit that uses a nonaffiliated third party as a service provider (and discloses personal information about an individual) must require that the third party implement and maintain reasonable security procedures and practices.

"Reasonable security procedures and practices" means data security procedures and practices developed, in good faith, and set forth in a written information security policy. "Personal information" means an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:

- a Social Security number;
- a driver's license number, State identification card number, or other individual identification number issued by a unit of State government;
- a passport number or other identification number issued by the United States government;
- an individual Taxpayer Identification Number; or
- a financial or other account number, credit card number, or credit card number that (in combination with a security code, access code, or password) would permit access to an individual's account.

Personal information does not include a voter registration number.

Department of Information Technology

DoIT and the Secretary of Information Technology are responsible for, among other things: (1) developing, maintaining, revising, and enforcing information technology (IT) policies, procedures, and standards; (2) providing technical assistance, advice, and recommendations to the Governor and any unit of State government concerning IT matters; (3) reviewing agency project plans to make information and services available to the public over the Internet; and (4) developing and maintaining a statewide IT Master Plan, as specified. "Information technology" means all electronic information processing, including maintenance, telecommunications, hardware, software, and associated services.

Public Information Act

Maryland's Public Information Act establishes that all persons are entitled to have access to information about the affairs of government and the official acts of public officials and employees. Each governmental unit that maintains public records must identify a representative whom a member of the public may contact to request a public record. OAG must post all such contact information on its website and in any *Public Information Act Manual* published by OAG.

Background: DoIT advises that the bill is necessary because the State currently lacks a comprehensive and consistent statutory framework governing how State agencies manage personal information. The existing patchwork of privacy rules has resulted in inconsistent protections for Maryland residents' sensitive information; unclear vendor obligations; overcollection (and over-retention) of personal data; lack of standardized processes for individuals to access, correct, or delete their data; and weak transparency and accountability for privacy practices across State government. The bill is intended to respond to these issues by codifying clear rules for data minimization, retention, deletion, vendor accountability, and individual rights.

State Expenditures: The Department of Budget and Management and DoIT advise that the bill can generally be implemented throughout State government with existing resources or with minimal additional costs, as many (though not all) of the requirements of the bill have already been implemented through Executive Order 01.01.2021.10.

However, some State agencies (*e.g.*, the Comptroller's Office, the Maryland Department of Transportation, and the Department of Disabilities) anticipate that the bill may result in an increased workload that cannot be handled by the agency's existing staff; notably, the existing Executive Order does not apply to the Comptroller's Office. While this analysis assumes that the bill can generally be implemented by most State agencies using existing budgeted resources (since the bill codifies many elements of the Executive Order), to the extent some agencies require additional staff to implement the bill, expenditures increase accordingly.

Additional Information

Recent Prior Introductions: Similar legislation has not been introduced within the last three years.

Designated Cross File: None.

Information Source(s): Department of Information Technology; Office of the Attorney General; Comptroller's Office; Judiciary (Administrative Office of the Courts); Maryland Higher Education Commission; University System of Maryland; Department of Budget and Management; Maryland Department of Disabilities; Maryland Department of Health; Department of Housing and Community Development; Department of Human Services; Maryland Department of Labor; Department of Public Safety and Correctional Services; Department of State Police; Maryland Department of Transportation; Department of Veterans and Military Families; Maryland Municipal League; Department of Legislative Services

Fiscal Note History: First Reader - February 8, 2026
me/rld

Analysis by: Eric F. Pierce

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

ANALYSIS OF ECONOMIC IMPACT ON SMALL BUSINESSES

TITLE OF BILL: Maryland Data Privacy and Protection Act of 2026

BILL NUMBER: HB 264

PREPARED BY: Sara Elalamy - DoIT - Legislative Director

PART A. ECONOMIC IMPACT RATING

This agency estimates that the proposed bill:

_X_ WILL HAVE MINIMAL OR NO ECONOMIC IMPACT ON MARYLAND SMALL BUSINESS

OR

WILL HAVE MEANINGFUL ECONOMIC IMPACT ON MARYLAND SMALL BUSINESSES

PART B. ECONOMIC IMPACT ANALYSIS

The bill is not expected to impose additional costs on state agencies or local governments.