Chapter 435

(House Bill 264)

AN ACT concerning

Maryland Data Privacy and Protection Act of 2026

FOR the purpose of limiting the personal information that may be collected, maintained, processed, and retained by units of State government under certain circumstances; requiring certain personal information to be deleted or de–identified under certain circumstances; requiring each unit to post a certain privacy notice on its Internet website and establishing certain requirements for privacy notices and privacy policies; requiring each unit of State government to designate a Privacy Officer; requiring the Department of Information Technology to establish certain requirements to be included in certain contracts; altering the definition of "personal information" as it relates to protection of information by government agencies; and generally relating to data privacy, protection, and transparency in State government.

BY repealing and reenacting, without amendments,
Article – Commercial Law
Section 14–4701(gg)
Annotated Code of Maryland
(2025 Replacement Volume)

BY repealing and reenacting, with amendments,
Article – General Provisions
Section 4–501
Annotated Code of Maryland
(2019 Replacement Volume and 2025 Supplement)

BY adding to
Article – State Finance and Procurement
Section 3.5–319
Annotated Code of Maryland
(2021 Replacement Volume and 2025 Supplement)

BY repealing and reenacting, with amendments,
Article – State Finance and Procurement
Section 13–115
Annotated Code of Maryland
(2021 Replacement Volume and 2025 Supplement)

BY repealing and reenacting, without amendments,
Article – State Government
Section 10–1301(a)

Annotated Code of Maryland
(2021 Replacement Volume and 2025 Supplement)

BY repealing and reenacting, with amendments,
Article – State Government
Section 10–1301(c) and 10–1702
Annotated Code of Maryland
(2021 Replacement Volume and 2025 Supplement)

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That the Laws of Maryland read as follows:

Article – Commercial Law

14–4701.

(gg) "Sensitive data" means personal data that includes:

(1) Data revealing:

(i) Racial or ethnic origin;

(ii) Religious beliefs;

(iii) Consumer health data;

(iv) Sex life;

(v) Sexual orientation;

(vi) Status as transgender or nonbinary;

(vii) National origin; or

(viii) Citizenship or immigration status;

(2) Genetic data or biometric data;

(3) Personal data of a consumer that the controller knows or has reason to know is a child; or

(4) Precise geolocation data.

Article – General Provisions

4–501.

(a) In this section, "personal record" means a public record that names or, with reasonable certainty, otherwise identifies an individual by an identifying factor such as:

(1) an address;

(2) a description;

(3) a fingerprint or voice print;

(4) a number; or

(5) a picture.

(b) (1) Personal records may not be created unless the need for the information has been clearly established by the unit collecting the records.

(2) Personal information collected for personal records:

(i) shall be appropriate and relevant to the **[**purposes**]** **LEGITIMATE GOVERNMENT PURPOSE** for which it is collected;

(II) SHALL BE LIMITED TO THE MINIMUM AMOUNT OF PERSONAL INFORMATION NECESSARY TO ACCOMPLISH THE LEGITIMATE GOVERNMENT PURPOSE FOR WHICH IT WAS COLLECTED;

[(ii)**] (III)** shall be accurate and current to the greatest extent practicable; **[**and**]**

(IV) SHALL NOT BE RETAINED FOR LONGER THAN IS REASONABLY NECESSARY TO FULFILL THE LEGITIMATE GOVERNMENT PURPOSE FOR WHICH IT WAS COLLECTED;

(V) IN ACCORDANCE WITH THE UNIT'S RETENTION SCHEDULE OR AS ALLOWED BY LAW, SHALL BE SECURELY DELETED OR DE–IDENTIFIED WHEN NO LONGER NEEDED TO FULFILL THE LEGITIMATE GOVERNMENT PURPOSE FOR WHICH IT WAS COLLECTED; AND

[(iii)**] (VI)** may not be obtained by fraudulent means.

(c) (1) This subsection applies only to units of the State.

(2) Except as otherwise provided by law, an official custodian who keeps personal records shall collect, to the greatest extent practicable, personal information from the person in interest.

(3) An official custodian who requests personal information for personal records shall provide the following information to each person in interest from whom personal information is collected:

(i) the **LEGITIMATE GOVERNMENT** purpose for which the personal information is collected;

(ii) any specific consequences to the person for refusal to provide the personal information;

(iii) the person's right to inspect, amend, or correct personal records, if any;

(iv) whether the personal information is generally available for public inspection; and

(v) whether the personal information is made available or transferred to or shared with any entity other than the official custodian.

(4) **(I)** Each unit of the State shall post **A PRIVACY NOTICE AND** its privacy policies on the collection of personal information, including the policies specified in this subsection, on its Internet website.

(II) THE PRIVACY NOTICE AND PRIVACY POLICIES POSTED UNDER SUBPARAGRAPH (I) OF THIS PARAGRAPH SHALL BE CONSISTENT WITH THE GUIDELINES, STANDARDS, AND POLICIES ISSUED BY THE DEPARTMENT OF INFORMATION TECHNOLOGY UNDER § 3.5–319 OF THE STATE FINANCE AND PROCUREMENT ARTICLE.

(5) The following personal records are exempt from the requirements of this subsection:

(i) information concerning the enforcement of criminal laws or the administration of the penal system;

(ii) information contained in investigative materials kept for the purpose of investigating a specific violation of State law and maintained by a State agency whose principal function may be other than law enforcement;

(iii) information contained in public records that are accepted by the State Archivist for deposit in the Maryland Hall of Records;

(iv) information gathered as part of formal research projects previously reviewed and approved by federally mandated institutional review boards; **[**and**]**

(V) INFORMATION CONTAINED IN APPLICATION OR RENEWAL MATERIALS RELATING TO THE LICENSING, REGISTRATION, OR CERTIFICATION OF AN INDIVIDUAL FOR AN OCCUPATION OR PROFESSION; AND

[(v)**] (VI)** any other personal records exempted by regulations adopted by the Secretary of Budget and Management, based on the recommendation of the Secretary of Information Technology.

(d) (1) This subsection does not apply to:

(i) a unit in the Legislative Branch of the State government;

(ii) a unit in the Judicial Branch of the State government; or

(iii) a board of license commissioners.

(2) If a unit or an instrumentality of the State keeps personal records, the unit or instrumentality shall submit an annual report to the Secretary of General Services.

(3) An annual report shall state:

(i) the name of the unit or instrumentality;

(ii) for each set of personal records:

1. the name of the set;

2. the location of the set; and

3. if a subunit keeps the set, the name of the subunit;

(iii) for each set of personal records that has not been previously reported:

1. the category of individuals to whom the set applies;

2. a brief description of the types of information that the set contains;

3. the major uses and purposes of the information;

4. by category, the source of information for the set; and

5. the policies and procedures of the unit or instrumentality as to:

A. access and challenges to the personal record by the person in interest; and

B. storage, retrieval, retention, disposal, and security, including controls on access; and

(iv) for each set of personal records that has been disposed of or changed significantly since the unit or instrumentality last submitted a report, the information required under item (iii) of this paragraph.

(4) A unit or an instrumentality that has two or more sets of personal records may combine the personal records in the report only if the character of the personal records is highly similar.

(5) The Secretary of General Services shall adopt regulations that govern the form and method of reporting under this subsection.

(6) The annual report shall be available for public inspection.

(e) The official custodian may allow inspection of personal records for which inspection otherwise is not authorized by a person who is engaged in a research project if:

(1) the researcher submits to the official custodian a written request that:

(i) describes the purpose of the research project;

(ii) describes the intent, if any, to publish the findings;

(iii) describes the nature of the requested personal records;

(iv) describes the safeguards that the researcher would take to protect the identity of the persons in interest; and

(v) states that persons in interest will not be contacted unless the official custodian approves and monitors the contact;

(2) the official custodian is satisfied that the proposed safeguards will prevent the disclosure of the identity of persons in interest; and

(3) the researcher makes an agreement with the unit or instrumentality that:

(i) defines the scope of the research project;

(ii) sets out the safeguards for protecting the identity of the persons in interest; and

(iii) states that a breach of any condition of the agreement is a breach of contract.

Article – State Finance and Procurement

3.5–319.

(A) EACH UNIT OF STATE GOVERNMENT SHALL DESIGNATE A PRIVACY OFFICER TO OVERSEE COMPLIANCE WITH THIS SUBTITLE AND COORDINATE WITH THE DEPARTMENT AND THE OFFICE OF THE ATTORNEY GENERAL.

(B) THE DEPARTMENT SHALL ADOPT REGULATIONS, GUIDANCE, AND MODEL TEMPLATES TO SUPPORT COMPLIANCE WITH THIS SUBTITLE, INCLUDING STANDARD PUBLIC INFORMATION ACT FORMATS AND DATA PROTECTION PROTOCOLS.

13–115.

(a) The Department of Information Technology shall require basic security**, DATA COLLECTION, AND PRIVACY** requirements to be included in a contract**[**:

(1) in**]** **UNDER** which a third–party contractor will**:**

(1) have access to and use State **[**telecommunication**]** **INFORMATION TECHNOLOGY** equipment, systems, or services; **[**or**]**

(2) COLLECT, STORE, OR PROCESS PERSONAL INFORMATION AS DEFINED IN § 10–1301 OF THE STATE GOVERNMENT ARTICLE; OR

[(2)**] (3) [**for systems or devices that will**]** connect to State **[**telecommunication**]** **INFORMATION TECHNOLOGY** equipment, systems, or services.

(b) The security requirements developed under subsection (a) of this section shall be consistent with a widely recognized security standard, including National Institute of Standards and Technology SP 800–171, ISO27001, or Cybersecurity Maturity Model Certification.

(C) THE PRIVACY REQUIREMENTS DEVELOPED UNDER SUBSECTION (A) OF THIS SECTION SHALL BE CONSISTENT WITH WIDELY RECOGNIZED PRIVACY STANDARDS, INCLUDING NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

(NIST) SP PRIVACY FRAMEWORK V1, NIST 800 SP 800–53 V5, AND NIST 800–207 SP ZERO TRUST ARCHITECTURE, AS THEY MAY BE UPDATED FROM TIME TO TIME.

Article – State Government

10–1301.

(a) In this subtitle the following words have the meanings indicated.

(c) (1) "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:

(i) a Social Security number**, AN INDIVIDUAL TAXPAYER IDENTIFICATION NUMBER, A PASSPORT NUMBER, OR OTHER IDENTIFICATION NUMBER ISSUED BY THE UNITED STATES GOVERNMENT**;

(ii) a driver's license number, state identification card number, or other individual identification number issued by a unit;

[(iii) a passport number or other identification number issued by the United States government;

(iv) an Individual Taxpayer Identification Number; or**]**

[(v)**] (III)** a financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account**;**

(IV) 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;

(V) GENETIC AND HEALTH–RELATED DATA, INCLUDING MENTAL HEALTH, SUBSTANCE USE DISORDER, AND DISABILITY; OR

(VI) SENSITIVE DATA, AS DEFINED IN § 14–4701 OF THE COMMERCIAL LAW ARTICLE.

(2) "Personal information" does not include a voter registration number.

10–1702.

(a) (1) In this section the following words have the meanings indicated.

(2) "Governmental entity" means a unit or instrumentality of State or local government.

(3) "Personal record" has the meaning stated in § 4–501 of the General Provisions Article.

(4) "SENSITIVE DATA" HAS THE MEANING STATED IN § 14–4701 OF THE COMMERCIAL LAW ARTICLE.

(b) (1) Subject to paragraph (2) of this subsection, on or before July 1, 2026, each governmental entity, in consultation with the Department of Information Technology, shall develop and publish procedures that prevent the sale and redisclosure of personal records and geolocation data provided or made available by the governmental entity in a way that harms the privacy of residents of the State.

(2) The procedures required and published under paragraph (1) of this subsection shall address:

(i) any possible contractual limitations on the sale or redisclosure of personal records or geolocation data that a governmental entity may place on a person who receives personal records or geolocation data that are provided or made available by the governmental entity;

(ii) considerations regarding:

1. the threat to privacy posed by data brokers who utilize personal records or geolocation data for commercial purposes;

2. the risk that personal records or geolocation data may be used for purposes other than the purposes for which the personal records or geolocation data were developed or collected; and

3. geolocation, genetic, and other sensitive data; and

(iii) any other considerations necessary to:

1. protect the privacy of residents of the State;

2. discourage the development of a secondary commercial market for personal records or geolocation data that are provided or made available by a governmental entity; and

3. limit a person who receives personal records or geolocation data that are provided or made available by a governmental entity from selling or redisclosing the data with other persons.

(c) On or before July 1, 2026, each governmental entity shall, in accordance with § 2–1257 of this article, submit to the General Assembly a copy of the procedures developed under subsection (b) of this section.

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2026.

Approved by the Governor, May 12, 2026.