

HOUSE BILL 264

S2

(PRE-FILED)

6lr0274

CF 6lr0273

By: Chair, Government, Labor, and Elections Committee (By Request – Departmental – Information Technology)

Requested: October 1, 2025

Introduced and read first time: January 14, 2026

Assigned to: Government, Labor, and Elections

A BILL ENTITLED

1 AN ACT concerning

2 **Maryland Data Privacy and Protection Act of 2026**

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

14 BY repealing and reenacting, without amendments,
15 Article – Commercial Law
16 Section 14–4701(gg)
17 Annotated Code of Maryland
18 (2025 Replacement Volume)

19 BY repealing and reenacting, with amendments,
20 Article – General Provisions
21 Section 4–501
22 Annotated Code of Maryland
23 (2019 Replacement Volume and 2025 Supplement)

24 BY adding to
25 Article – State Finance and Procurement
26 Section 3.5–319

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



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

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

repealing and reenacting, without amendments,
Article – State Government
Section 10–1301(a)
Annotated Code of Maryland
(2021 Replacement Volume and 2025 Supplement)

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

21 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 hold; or
- (4) Precise geolocation data.

Article – General Provisions

6 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.

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

16 (2) Personal information collected for personal records:

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

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

22 [(ii)] (III) shall be accurate and current to the greatest extent
23 practicable: [and]

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

27 (v) IN ACCORDANCE WITH THE UNIT'S RETENTION SCHEDULE
28 OR AS ALLOWED BY LAW, SHALL BE SECURELY DELETED OR DE-IDENTIFIED WHEN

1 **NO LONGER NEEDED TO FULFILL THE LEGITIMATE GOVERNMENT PURPOSE FOR**
2 **WHICH IT WAS COLLECTED; AND**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4 (iii) information contained in public records that are accepted by the
5 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]

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

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

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

17 (iii) a board of license commissioners.

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

20 (3) An annual report shall state:

21 (i) the name of the unit or instrumentality;

22 (ii) for each set of personal records:

23 1. the name of the set;

24 2. the location of the set; and

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

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

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

- A. access and challenges to the personal record by the person
- B. storage, retrieval, retention, disposal, and security, less; and

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

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

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

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

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

23 (i) describes the purpose of the research project;

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

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

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

28 (v) states that persons in interest will not be contacted unless the
29 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 (3) the researcher makes an agreement with the unit or instrumentality
4 that:

5 (i) defines the scope of the research project;

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

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

Article – State Finance and Procurement

11 3.5-319.

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

19 13-115.

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

22 (1) in] UNDER which a third-party contractor will:

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

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

27 [27] (3) [for systems or devices that will] connect to State
28 [telecommunication] INFORMATION TECHNOLOGY equipment, systems, or services.

1 Standards and Technology SP 800–171, ISO27001, or Cybersecurity Maturity Model
2 Certification.

3 **(C) THE PRIVACY REQUIREMENTS DEVELOPED UNDER SUBSECTION (A) OF**
4 **THIS SECTION SHALL BE CONSISTENT WITH WIDELY RECOGNIZED PRIVACY**
5 **STANDARDS, INCLUDING NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**
6 **(NIST) SP PRIVACY FRAMEWORK V1, NIST 800 SP 800–53 V5, AND NIST 800–207**
7 **SP ZERO TRUST ARCHITECTURE, AS THEY MAY BE UPDATED FROM TIME TO TIME.**

8 **Article – State Government**

9 10–1301.

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

11 (c) (1) “Personal information” means an individual’s first name or first initial
12 and last name, personal mark, or unique biometric or genetic print or image, in combination
13 with one or more of the following data elements:

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

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

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

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

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

25 **(IV) A USERNAME OR E-MAIL ADDRESS IN COMBINATION WITH A**
26 **PASSWORD OR SECURITY QUESTION AND ANSWER THAT PERMITS ACCESS TO AN**
27 **INDIVIDUAL’S E-MAIL ACCOUNT;**

28 **(V) GENETIC AND HEALTH-RELATED DATA, INCLUDING**
29 **MENTAL HEALTH, SUBSTANCE USE DISORDER, AND DISABILITY; OR**

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

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

2 10-1702.

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

4 (2) "Governmental entity" means a unit or instrumentality of State or local
5 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.

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

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

21 (ii) considerations regarding:

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

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

28 (iii) any other considerations necessary to:

29 1. protect the privacy of residents of the State;

4 (c) On or before July 1, 2026, each governmental entity shall, in accordance with
5 § 2-1257 of this article, submit to the General Assembly a copy of the procedures developed
6 under subsection (b) of this section.

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