

SENATE BILL 504

I3, S2, E4

6lr2052
CF HB 711

By: **Senator Lam**

Introduced and read first time: February 2, 2026

Assigned to: Finance

Committee Report: Favorable with amendments

Senate action: Adopted

Read second time: March 24, 2026

CHAPTER _____

1 AN ACT concerning

2 **Data Privacy – Consumer Data, Public Records, and Message Switching System**
3 **(Data Privacy Act)**

4 FOR the purpose of prohibiting a certain controller from knowingly selling the personal
5 data of a consumer ~~if the controller knew or should have known that the purchaser~~
6 ~~seeks to use the data for immigration enforcement~~ to a certain governmental unit
7 that has engaged in or supported civil immigration enforcement under certain
8 circumstances; altering the manner in which certain provisions of law may be
9 construed with respect to a controller's or processor's compliance with governmental
10 actions; requiring a custodian of a public record to adopt reasonable rules and
11 regulations that prevent unauthorized disclosure or inspection of a public record,
12 and to take reasonable steps to determine whether a public record is accessed for
13 enforcing immigration law; altering the reasons for which a public record may be
14 denied from being disclosed or inspected; requiring an entity that operates a certain
15 message switching system to take certain actions regarding system access; requiring
16 certain procedures developed and published by certain governmental entities to
17 account for certain sensitive data ~~containing certain sensitive attributes~~; and
18 generally relating to data privacy of individuals in the State.

19 BY repealing and reenacting, without amendments,
20 Article – Commercial Law
21 Section 14-4701(a), ~~(w)~~, and ~~(y)~~ and (w)
22 Annotated Code of Maryland
23 (2025 Replacement Volume)

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.

Underlining indicates amendments to bill.

~~Strike out~~ indicates matter stricken from the bill by amendment or deleted from the law by amendment.



- 1 BY adding to
 2 Article – Commercial Law
 3 Section 14–4701(p–1)
 4 Annotated Code of Maryland
 5 (2025 Replacement Volume)
- 6 BY repealing and reenacting, with amendments,
 7 Article – Commercial Law
 8 Section 14–4701(x), (cc), and (gg), ~~and (hh) through (jj)~~, 14–4703(b)(8), 14–4707(a),
 9 and 14–4712(a)
 10 Annotated Code of Maryland
 11 (2025 Replacement Volume)
- 12 ~~BY adding to~~
 13 ~~Article – Commercial Law~~
 14 ~~Section 14–4701(hh)~~
 15 ~~Annotated Code of Maryland~~
 16 ~~(2025 Replacement Volume)~~
- 17 BY repealing and reenacting, with amendments,
 18 Article – General Provisions
 19 Section 4–201, 4–320(b) and (g)(2), and 4–320.1
 20 Annotated Code of Maryland
 21 (2019 Replacement Volume and 2025 Supplement)
- 22 BY repealing and reenacting, with amendments,
 23 Article – Public Safety
 24 Section 3–529
 25 Annotated Code of Maryland
 26 (2022 Replacement Volume and 2025 Supplement)
- 27 BY repealing and reenacting, with amendments,
 28 Article – State Government
 29 Section 10–1702
 30 Annotated Code of Maryland
 31 (2021 Replacement Volume and 2025 Supplement)

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

34 **Article – Commercial Law**

35 14–4701.

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

37 **(P–1) “DIVISION” HAS THE MEANING STATED IN § 13–101 OF THIS ARTICLE.**

1 (w) (1) "Personal data" means any information that is linked or can be
2 reasonably linked to an identified or identifiable consumer.

3 (2) "Personal data" does not include:

4 (i) De-identified data; or

5 (ii) Publicly available information.

6 (x) (1) "Precise geolocation data" means information derived from technology
7 that can precisely and accurately identify, **WITHIN A RADIUS OF 1,750 FEET**, the specific
8 location of a consumer [within a radius of 1,750 feet], **A MOBILE DEVICE, OR A VEHICLE.**

9 (2) "Precise geolocation data" includes global positioning system level
10 latitude and longitude coordinates or other similar mechanisms.

11 (3) "Precise geolocation data" does not include:

12 (i) The content of communications;

13 (ii) Data generated by or connected to an advanced utility metering
14 infrastructure system; or

15 (iii) Data generated by equipment used by a utility company.

16 ~~(y) (1) "Process" means an operation or set of operations performed by manual
17 or automated means on personal data.~~

18 ~~(2) "Process" includes collecting, using, storing, disclosing, analyzing,
19 deleting, or modifying personal data.~~

20 (cc) (1) "Publicly available information" means information that a person:

21 (i) Lawfully obtains from a record of a governmental entity, **IF THE**
22 **PERSON PROCESSES THE INFORMATION IN ACCORDANCE WITH EACH**
23 **RESTRICTION OR TERM OF USE PLACED ON THE INFORMATION BY THAT THE**
24 **GOVERNMENTAL ENTITY IMPOSES AS A CONDITION FOR PROVIDING THE**
25 **INFORMATION TO THE PERSON;**

26 (ii) Reasonably believes a consumer or widely distributed media
27 have lawfully made available to the general public; or

28 (iii) If the consumer has not restricted the information to a specific
29 audience, obtains from a person to whom the consumer disclosed the information.

(2) “Publicly available information” does not include biometric data collected by a business about a consumer without the consumer’s knowledge.

(gg) **(1)** “Sensitive ~~{data}~~” means personal data that includes] ~~ATTRIBUTE”~~
~~MEANS:~~

~~(1)~~ **(I)** Data revealing:

~~(i)~~ **1.** Racial or ethnic origin;

~~(ii)~~ **2.** Religious beliefs;

~~(iii)~~ **3.** Consumer health data;

~~(iv)~~ **4.** Sex life;

~~(v)~~ **5.** Sexual orientation;

~~(vi)~~ **6.** Status as transgender or nonbinary;

~~(vii)~~ **7.** National origin; or

~~(viii)~~ **8.** Citizenship or immigration status;

~~(2)~~ **(II)** Genetic data or biometric data;

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

~~(4)~~ **(IV)** Precise geolocation data.

(2) “SENSITIVE DATA” INCLUDES DATA INFERRED BY A CONTROLLER BASED ON PERSONAL DATA THAT, ALONE OR IN COMBINATION WITH OTHER DATA, IS USED TO INDICATE ANY DATA DESCRIBED UNDER PARAGRAPH (1)(I) THROUGH (IV) OF THIS SUBSECTION.

~~**(III) “SENSITIVE DATA” MEANS PERSONAL DATA THAT INCLUDES A SENSITIVE ATTRIBUTE OR ANY OTHER PERSONAL DATA PROCESSED FOR THE PURPOSE OF IDENTIFYING A SENSITIVE ATTRIBUTE.**~~

~~**[(hh)](II) (1) “Targeted advertising” means displaying advertisements to a consumer or on a device identified by a unique identifier, where the advertisement is selected based on personal data obtained or inferred from the consumer’s activities over time and across nonaffiliated websites or online applications that are unaffiliated with each other, in order to predict the consumer’s preferences or interests.**~~

1 ~~(2) “Targeted advertising” does not include:~~

2 ~~(i) Advertisements based on the context of a consumer’s current~~
3 ~~search query, visit to a website, or online application;~~

4 ~~(ii) Advertisements based on a consumer’s activities within a~~
5 ~~controller’s websites or online applications;~~

6 ~~(iii) Advertisements directed to a consumer in response to the~~
7 ~~consumer’s request for information or feedback; or~~

8 ~~(iv) Processing personal data solely to measure or report advertising~~
9 ~~frequency, performance, or reach.~~

10 ~~[(i)] (JJ) “Third party” means a person other than the relevant consumer,~~
11 ~~controller, processor, or affiliate of the controller or processor of relevant personal data.~~

12 ~~[(j)] (KK) “Trade secret” has the meaning stated in § 11-1201 of this article.~~

13 14-4703.

14 (b) The following information and data are exempt from this subtitle:

15 (8) Personal data collected, processed, sold, or disclosed [in compliance] ~~TO~~
16 ~~THE EXTENT NECESSARY TO COMPLY with~~ AS REQUIRED BY the federal Driver’s
17 Privacy Protection Act of 1994;

18 14-4707.

19 (a) A controller may not:

20 (1) Except where the collection or processing is strictly necessary to provide
21 or maintain a specific product or service requested by the consumer to whom the personal
22 data pertains, collect, process, or share sensitive data concerning a consumer;

23 (2) Sell sensitive data;

24 (3) Process personal data in violation of State or federal laws that prohibit
25 unlawful discrimination;

26 (4) Process the personal data of a consumer for the purposes of targeted
27 advertising if the controller knew or should have known that the consumer is under the age
28 of 18 years;

29 (5) Sell the personal data of a consumer if the controller knew or should
30 have known that ~~the~~;

1 ~~(I)~~ ~~THE~~ consumer is under the age of 18 years; ~~OR~~

2 ~~(II)~~ ~~THE PURCHASER SEEKS TO USE THE PERSONAL DATA FOR~~
3 ~~THE PURPOSE OF IMMIGRATION ENFORCEMENT;~~

4 (6) KNOWINGLY SELL THE PERSONAL DATA OF A CONSUMER TO A
5 FEDERAL, STATE, OR LOCAL GOVERNMENTAL UNIT THAT, WITHIN THE 6 MONTHS
6 THAT IMMEDIATELY PRECEDE THE SALE OF THE PERSONAL DATA, HAS ENGAGED IN
7 OR SUPPORTED CIVIL IMMIGRATION ENFORCEMENT THROUGH THE PROVISION OF
8 PERSONNEL OR MATERIAL RESOURCES.

9 (7) Discriminate against a consumer for exercising a consumer right
10 contained in this subtitle, including denying goods or services, charging different prices or
11 rates for goods or services, or providing a different level of quality of goods or services to
12 the consumer;

13 ~~(7)~~ (8) Collect, process, or transfer personal data or publicly available
14 data in a manner that unlawfully discriminates in or otherwise unlawfully makes
15 unavailable the equal enjoyment of goods or services on the basis of race, color, religion,
16 national origin, sex, sexual orientation, gender identity, or disability, unless the collection,
17 processing, or transfer of personal data is for:

18 (i) The controller's self-testing to prevent or mitigate unlawful
19 discrimination;

20 (ii) The controller's diversifying of an applicant, participant, or
21 customer pool; or

22 (iii) A private club or group not open to the public, as described in §
23 201(e) of the Civil Rights Act of 1964; or

24 ~~(8)~~ (9) Unless the controller obtains the consumer's consent, process
25 personal data for a purpose that is neither reasonably necessary to, nor compatible with,
26 the disclosed purposes for which the personal data is processed, as disclosed to the
27 consumer.

28 14-4712.

29 (a) (1) Nothing in this subtitle may be construed to restrict a controller's or
30 processor's ability to:

31 ~~(1)~~ (I) Comply with federal, State, or local laws or regulations;

32 ~~(2)~~ (II) ~~Comply~~ EXCEPT AS PROVIDED IN PARAGRAPH (2) OF THIS
33 SUBSECTION, COMPLY with a civil, criminal, or regulatory ~~inquiry, investigation,~~

1 subpoena, or summons by a federal, State, local, or other governmental authority, ~~EXCEPT~~
2 ~~TO THE EXTENT THAT AN INQUIRY, AN INVESTIGATION, A SUBPOENA, OR A SUMMONS~~
3 ~~PERTAINS SOLELY TO IMMIGRATION ENFORCEMENT;~~

4 ~~(3)~~ **(III)** ~~Cooperate~~ **EXCEPT AS PROVIDED IN PARAGRAPH (2) OF THIS**
5 **SUBSECTION, COOPERATE** with law enforcement agencies concerning conduct or activity
6 that the controller or processor reasonably and in good faith believes may violate federal,
7 State, or local laws or regulations;

8 ~~(4)~~ **(IV)** Investigate, establish, exercise, prepare for, or defend a legal
9 claim;

10 ~~(5)~~ **(V)** Provide a product or service specifically requested by a consumer;

11 ~~(6)~~ **(VI)** Perform under a contract to which a consumer is a party,
12 including fulfilling the terms of a written warranty;

13 ~~(7)~~ **(VII)** Take steps at the request of a consumer before entering into a
14 contract;

15 ~~(8)~~ **(VIII)** Take immediate steps to protect an interest that is essential for
16 the life or physical safety of a consumer or another individual and when the processing
17 cannot be manifestly based on another legal basis;

18 ~~(9)~~ **(IX)** Prevent, detect, protect against, investigate, prosecute those
19 responsible, or otherwise respond to a security incident, identity theft, fraud, harassment,
20 malicious or deceptive activity, or any other type of illegal activity;

21 ~~(10)~~ **(X)** Preserve the integrity or security of systems; or

22 ~~(11)~~ **(XI)** Assist another controller, processor, or third party with an
23 obligation under this subtitle.

24 **(2) (I) THIS PARAGRAPH DOES NOT APPLY IF A CONTROLLER OR**
25 **PROCESSOR IS PRESENTED WITH A VALID WARRANT ISSUED BY A FEDERAL OR**
26 **STATE COURT THAT PARTICULARLY DESCRIBES THE PERSONAL DATA TO BE**
27 **ACCESSED.**

28 **(II) PARAGRAPH (1)(II) OF THIS SUBSECTION DOES NOT APPLY**
29 **TO A CONTROLLER'S OR PROCESSOR'S COMPLIANCE WITH A SUBPOENA OR**
30 **SUMMONS THAT IS DERIVED FROM A FEDERAL, STATE, OR LOCAL GOVERNMENTAL**
31 **UNIT THAT, WITHIN THE 6 MONTHS THAT IMMEDIATELY PRECEDE THE ISSUANCE OF**
32 **THE SUBPOENA OR SUMMONS, HAS ENGAGED IN OR SUPPORTED CIVIL IMMIGRATION**
33 **ENFORCEMENT THROUGH THE PROVISION OF PERSONNEL OR MATERIAL**
34 **RESOURCES.**

1 **(III) PARAGRAPH (1)(III) OF THIS SUBSECTION DOES NOT APPLY**
 2 **TO A CONTROLLER OR PROCESSOR THAT KNOWS THE LAW ENFORCEMENT AGENCY**
 3 **REQUESTING THE COOPERATION HAS, WITHIN THE 6 MONTHS THAT IMMEDIATELY**
 4 **PRECEDE THE REQUEST FOR COOPERATION, ENGAGED IN OR SUPPORTED CIVIL**
 5 **IMMIGRATION ENFORCEMENT THROUGH THE PROVISION OF PERSONNEL OR**
 6 **MATERIAL RESOURCES.**

7 **(IV) THE DIVISION MAY POST MATERIALS ON ITS WEBSITE TO**
 8 **PROVIDE CONSUMER EDUCATION AND OTHER RESOURCES REGARDING CIVIL**
 9 **IMMIGRATION ENFORCEMENT.**

10 **Article – General Provisions**

11 4–201.

12 (a) (1) Except as otherwise provided by law, a custodian shall allow a person
 13 or governmental unit to inspect any public record at any reasonable time.

14 (2) Inspection or copying of a public record may be denied only to the extent
 15 provided under this title.

16 (b) To protect public records and to prevent unnecessary interference with official
 17 business, each official custodian shall adopt reasonable rules or regulations that, subject to
 18 this title[,]:

19 **(1) govern timely production and inspection of a public record; AND**

20 **(2) PREVENT UNAUTHORIZED DISCLOSURE OR INSPECTION OF A**
 21 **PUBLIC RECORD, INCLUDING IN ACCORDANCE WITH § 4–320.1 OF THIS TITLE.**

22 (c) Each official custodian shall:

23 (1) designate types of public records of the governmental unit that are to
 24 be made available to any applicant immediately on request; and

25 (2) maintain a current list of the types of public records that have been
 26 designated as available to any applicant immediately on request.

27 4–320.

28 (b) Except as provided in subsections (c) through (f) of this section, **AND SUBJECT**
 29 **TO § 4–320.1 OF THIS SUBTITLE**, a custodian may not knowingly disclose a public record
 30 of the Motor Vehicle Administration containing personal information.

1 (g) (2) A person receiving personal information under subsection (d), (e), or (f)
2 of this section may not disclose the personal information to a [federal agent] PERSON or
3 [federal] GOVERNMENT agency for the purpose of [federal] immigration enforcement
4 unless the person is presented with a valid warrant issued by a federal court or a court of
5 this State.

6 4-320.1.

7 (a) In this section, “facial recognition” means a biometric software application
8 that identifies or verifies a person by comparing and analyzing patterns based on a person’s
9 facial contours.

10 (b) **A CUSTODIAN SHALL TAKE REASONABLE STEPS TO DETERMINE**
11 **WHETHER A PERSON SEEKING ACCESS TO A PUBLIC RECORD IS DOING SO FOR THE**
12 **PURPOSE OF ENFORCING IMMIGRATION LAW.**

13 (c) (1) Notwithstanding any other provision of this title[, an officer, an
14 employee, an agent, or a contractor of the State or a political subdivision] **A CUSTODIAN**
15 shall deny inspection of the part of a public record that contains personal information or
16 inspection of a photograph of an individual by any [federal agency] PERSON seeking access
17 for the purpose of enforcing [federal] immigration law, unless the [officer, employee, agent,
18 or contractor] CUSTODIAN is provided with a valid warrant issued by a federal court or a
19 court of this State **THAT ~~CLEARLY IDENTIFIES~~ PARTICULARLY DESCRIBES THE**
20 **RECORD TO BE ACCESSED.**

21 (2) Notwithstanding any other provision of this title[, an officer, an
22 employee, an agent, or a contractor of the State or a political subdivision] **A CUSTODIAN**
23 shall deny inspection using a facial recognition search of a digital photographic image or
24 actual stored data of a digital photographic image by any [federal agency] PERSON seeking
25 access for the purpose of enforcing [federal] immigration law, unless the [officer, employee,
26 agent, or contractor] CUSTODIAN is provided with a valid warrant issued by a federal court
27 or a court of this State **THAT ~~CLEARLY IDENTIFIES~~ PARTICULARLY DESCRIBES THE**
28 **RECORD TO BE ACCESSED.**

29 (3) On or before June 1, 2023, and each June 1 thereafter, the Motor
30 Vehicle Administration, the Department of State Police, and the Department of Public
31 Safety and Correctional Services shall, with respect to requests from [federal]
32 GOVERNMENT agencies seeking access for the purpose of [federal] immigration
33 enforcement for personal information, a photograph of an individual, or a facial recognition
34 search, whether or not the request was initiated through a State or local law enforcement
35 agency, report to the General Assembly, in accordance with § 2-1257 of the State
36 Government Article, the following information for the immediately preceding calendar
37 year:

1 (i) the number of requests received from any [federal]
2 GOVERNMENT agency for personal information, a photograph of an individual, or a facial
3 recognition search;

4 (ii) the number of requests received from any [federal]
5 GOVERNMENT agency for personal information, a photograph of an individual, or a facial
6 recognition search for which a valid warrant issued by a federal court or a court of this
7 State was provided;

8 (iii) the number and purpose of facial recognition searches completed
9 for any [federal] GOVERNMENT agency based on personal information or a photograph of
10 an individual provided to the [federal] GOVERNMENT agency by the Motor Vehicle
11 Administration, the Department of State Police, or the Department of Public Safety and
12 Correctional Services; and

13 (iv) the number of individuals whose personal information or
14 photograph was provided to any [federal] GOVERNMENT agency by, respectively, the
15 Motor Vehicle Administration, the Department of State Police, and the Department of
16 Public Safety and Correctional Services.

17 **(D) THE MOTOR VEHICLE ADMINISTRATION, THE DEPARTMENT OF STATE**
18 **POLICE, AND THE DEPARTMENT OF PUBLIC SAFETY AND CORRECTIONAL**
19 **SERVICES SHALL ADOPT REGULATIONS AND PROCEDURES TO IMPLEMENT,**
20 **ENFORCE, AND ENSURE COMPLIANCE WITH THIS SECTION.**

21 Article – Public Safety

22 3–529.

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

24 (2) (i) “Database” means any database operated by State and local law
25 enforcement agencies, including databases maintained for a law enforcement agency by a
26 private vendor.

27 (ii) “Database” does not include a registry operated under Title 11,
28 Subtitle 7 of the Criminal Procedure Article.

29 (3) (i) “Law enforcement agency” means a federal, state, or local agency
30 authorized to enforce criminal laws.

31 (ii) “Law enforcement agency” includes the Maryland Department of
32 Public Safety and Correctional Services.

33 **(4) “MESSAGE SWITCHING SYSTEM” MEANS A LAW ENFORCEMENT**
34 **COMMUNICATIONS PLATFORM THAT AUTOMATICALLY ROUTES, FORMATS, AND**

1 **DELIVERS ELECTRONIC QUERIES AND RESPONSES BETWEEN LAW ENFORCEMENT**
2 **AGENCIES AND DATABASES.**

3 (b) An entity operating a database **OR A MESSAGE SWITCHING SYSTEM** shall:

4 (1) deny access to the database **OR MESSAGE SWITCHING SYSTEM** to any
5 **[individual] PERSON** who is seeking access for the purpose of enforcing **[federal]**
6 immigration law, unless the **[individual] PERSON** presents a valid warrant issued by a
7 federal court or a court of this State; and

8 (2) require an individual accessing the database **OR MESSAGE**
9 **SWITCHING SYSTEM** to provide to the entity:

10 (i) the individual's name;

11 (ii) the individual's contact information, including a telephone
12 number, an e-mail address, and a physical address; and

13 (iii) unless the individual presents a valid warrant issued by a federal
14 court or a court of this State, a statement by the individual, under penalty of perjury, that
15 the individual is not accessing the database **OR MESSAGE SWITCHING SYSTEM** for the
16 purpose of enforcing **[federal]** immigration law.

17 **(C) EACH ENTITY OPERATING A DATABASE AND, WITH RESPECT TO A**
18 **MESSAGE SWITCHING SYSTEM, THE DEPARTMENT OF PUBLIC SAFETY AND**
19 **CORRECTIONAL SERVICES SHALL ADOPT REGULATIONS TO IMPLEMENT THIS**
20 **SECTION.**

21 **Article – State Government**

22 10–1702.

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

24 (2) “Governmental entity” means a unit or instrumentality of State or local
25 government.

26 (3) “Personal record” has the meaning stated in § 4–501 of the General
27 Provisions Article.

28 **(4) “SENSITIVE ~~ATTRIBUTE~~ DATA” HAS THE MEANING STATED IN §**
29 **14–4701 OF THE COMMERCIAL LAW ARTICLE.**

30 (b) (1) Subject to paragraph (2) of this subsection, on or before July 1, 2026,
31 each governmental entity, in consultation with the Department of Information Technology,
32 shall develop and publish procedures that prevent the sale and redisclosure of personal

1 records and [geolocation] SENSITIVE data ~~CONTAINING SENSITIVE ATTRIBUTES~~
2 provided or made available by the governmental entity in a way that harms the privacy of
3 residents of the State.

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

6 (i) any possible contractual limitations on the sale or redisclosure of
7 personal records or [geolocation] SENSITIVE data ~~CONTAINING SENSITIVE ATTRIBUTES~~
8 that a governmental entity may place on a person who receives personal records or
9 [geolocation] SENSITIVE data ~~CONTAINING SENSITIVE ATTRIBUTES~~ that are provided
10 or made available by the governmental entity;

11 (ii) considerations regarding:

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

14 2. the risk that personal records or [geolocation] SENSITIVE
15 data ~~CONTAINING SENSITIVE ATTRIBUTES~~ may be used for purposes other than the
16 purposes for which the personal records or [geolocation] SENSITIVE data ~~CONTAINING~~
17 ~~SENSITIVE ATTRIBUTES~~ were developed or collected; and

18 [3. geolocation, genetic, and other sensitive data; and]

19 (iii) any other considerations necessary to:

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

21 2. discourage the development of a secondary commercial
22 market for personal records or [geolocation] SENSITIVE data ~~CONTAINING SENSITIVE~~
23 ~~ATTRIBUTES~~ that are provided or made available by a governmental entity; and

24 3. limit a person who receives personal records or
25 [geolocation] SENSITIVE data ~~CONTAINING SENSITIVE ATTRIBUTES~~ that are provided
26 or made available by a governmental entity from selling or disclosing the data with other
27 persons.

28 (c) On or before July 1, 2026, each governmental entity shall, in accordance with
29 § 2–1257 of this article, submit to the General Assembly a copy of the procedures developed
30 under subsection (b) of this section.

31 SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect July
32 1, 2026.