

SENATE BILL 274

P1

0lr0126
CF HB 340

By: **The President (By Request – Administration) and Senators Bailey, Carozza, Cassilly, Eckardt, Edwards, Gallion, Hershey, Jennings, Kagan, Lam, Ready, Salling, Serafini, and West**

Introduced and read first time: January 20, 2020

Assigned to: Education, Health, and Environmental Affairs

A BILL ENTITLED

1 AN ACT concerning

2 **State Government – Protection of Information – Revisions**
3 **(Maryland Data Privacy Act)**

4 FOR the purpose of requiring certain units of State government to comply with certain
5 standards and guidelines to ensure that the security of all information systems and
6 applications is managed through a certain framework; requiring certain units of
7 State government to undertake activities comprising collection, processing, and
8 sharing of personally identifiable information in good faith; requiring certain units
9 to identify and document certain legal authority, describe a certain purpose and
10 make certain notifications, adopt a certain privacy governance and risk management
11 program, implement certain security measures, establish certain privacy
12 requirements and incorporate the requirements into certain agreements, take
13 certain steps, implement certain processes, and establish certain notice provisions;
14 requiring certain units to advise certain individuals whether certain information is
15 required to be provided by law or whether the provision is voluntary and subject to
16 certain discretion; requiring certain units to provide an individual with certain
17 means to access certain information and certain third parties; requiring certain units
18 to include certain means in certain notices and provide certain notices to individuals
19 at or before the point of sharing personally identifiable information; requiring certain
20 units to provide an individual with a certain process and the means to opt out of
21 sharing information with third parties under certain circumstances; authorizing the
22 Secretary of Information Technology to adopt certain regulations; establishing that
23 certain provisions of law do not apply to the University System of Maryland;
24 providing for the application and construction of certain provisions of law; providing
25 that certain provisions of this Act do not apply to the Office of the Attorney General;
26 defining certain terms; repealing certain definitions; making conforming changes;
27 and generally relating to the protection of personally identifiable information by
28 government agencies.

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.



1 BY repealing and reenacting, with amendments,
2 Article – State Government
3 Section 10–1301 through 10–1304 and 10–1305(a), (b)(1) and (2), (c)(1), (g)(1), (h)(2),
4 and (j)
5 Annotated Code of Maryland
6 (2014 Replacement Volume and 2019 Supplement)

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

9 **Article – State Government**

10 10–1301.

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

12 (b) “Encryption” means the protection of data in electronic or optical form, in
13 storage or in transit, using a technology that:

14 (1) is certified to meet or exceed the level that has been adopted by the
15 Federal Information Processing Standards issued by the National Institute of Standards
16 and Technology; and

17 (2) renders such data indecipherable without an associated cryptographic
18 key necessary to enable decryption of such data.

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

22 (i) a Social Security number;

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

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

27 (iv) an Individual Taxpayer Identification Number; or

28 (v) a financial or other account number, a credit card number, or a
29 debit card number that, in combination with any required security code, access code, or
30 password, would permit access to an individual’s account.

31 (2) “Personal information” does not include a voter registration number.

32 (d) “Reasonable security procedures and practices” means data security

1 procedures and practices developed, in good faith, and set forth in a written information
2 security policy.]

3 (C) "INDIVIDUAL" MEANS AN INDIVIDUAL WHO INTERACTS WITH A UNIT.

4 (D) (1) "PERSONALLY IDENTIFIABLE INFORMATION" MEANS
5 INFORMATION THAT CAN BE USED TO DISTINGUISH OR TRACE AN INDIVIDUAL'S
6 IDENTITY, EITHER ALONE OR WHEN COMBINED WITH OTHER INFORMATION
7 ASSOCIATED WITH A PARTICULAR INDIVIDUAL, INCLUDING:

8 (I) UNIQUE PERSONAL IDENTIFIERS, INCLUDING:

9 1. A FULL NAME;

10 2. A FIRST INITIAL AND LAST NAME;

11 3. A SOCIAL SECURITY NUMBER;

12 4. A DRIVER'S LICENSE NUMBER, A STATE
13 IDENTIFICATION NUMBER, OR ANY OTHER IDENTIFICATION NUMBER ISSUED BY A
14 UNIT; AND

15 5. A PASSPORT NUMBER;

16 (II) CHARACTERISTICS OF CLASSIFICATIONS PROTECTED
17 UNDER FEDERAL OR STATE LAW;

18 (III) BIOMETRIC INFORMATION INCLUDING AN INDIVIDUAL'S
19 PHYSIOLOGICAL, BIOLOGICAL, OR BEHAVIORAL CHARACTERISTICS, INCLUDING AN
20 INDIVIDUAL'S DEOXYRIBONUCLEIC ACID (DNA), THAT CAN BE USED, SINGLY OR IN
21 COMBINATION WITH EACH OTHER OR WITH OTHER IDENTIFYING DATA, TO
22 ESTABLISH INDIVIDUAL IDENTITY;

23 (IV) GEOLOCATION DATA;

24 (V) INTERNET OR OTHER ELECTRONIC NETWORK ACTIVITY
25 INFORMATION, INCLUDING BROWSING HISTORY, SEARCH HISTORY, AND
26 INFORMATION REGARDING AN INDIVIDUAL'S INTERACTION WITH AN INTERNET
27 WEBSITE, APPLICATION, OR ADVERTISEMENT;

28 (VI) INFORMATION FROM MULTIPLE SOURCES THAT WHEN USED
29 IN COMBINATION WITH EACH OTHER OR OTHER IDENTIFYING INFORMATION CAN BE
30 USED TO ESTABLISH INDIVIDUAL IDENTITY; AND

1 (VII) A FINANCIAL OR OTHER ACCOUNT NUMBER, A CREDIT CARD
2 NUMBER, OR A DEBIT CARD NUMBER THAT, IN COMBINATION WITH ANY REQUIRED
3 SECURITY CODE, ACCESS CODE, OR PASSWORD, WOULD PERMIT ACCESS TO AN
4 INDIVIDUAL'S ACCOUNT.

5 (2) "PERSONALLY IDENTIFIABLE INFORMATION" DOES NOT
6 INCLUDE:

7 (I) VOTER REGISTRATION INFORMATION;

8 (II) INFORMATION PUBLICLY DISCLOSED BY THE INDIVIDUAL
9 WITHOUT BEING UNDER DURESS OR COERCION; OR

10 (III) DATA RENDERED ANONYMOUS THROUGH THE USE OF
11 TECHNIQUES, INCLUDING OBFUSCATION, DELETION AND REDACTION, AND
12 ENCRYPTION, SO THAT THE INDIVIDUAL IS NO LONGER IDENTIFIABLE.

13 (E) "REASONABLE SECURITY PROCEDURES AND PRACTICES" MEANS
14 SECURITY PROTECTIONS THAT ALIGN WITH DEPARTMENT OF INFORMATION
15 TECHNOLOGY POLICIES AND THE FEDERAL INFORMATION SECURITY
16 MODERNIZATION ACT (FISMA) OF 2014.

17 [(e)] (F) "Records" means information that is inscribed on a tangible medium or
18 that is stored in an electronic or other medium and is retrievable in perceivable form.

19 [(f)] (G) "Unit" means:

20 (1) an executive agency, or a department, a board, a commission, an
21 authority, a public institution of higher education, a unit or an instrumentality of the State;
22 or

23 (2) a county, municipality, bi-county, regional, or multicounty agency,
24 county board of education, public corporation or authority, or any other political subdivision
25 of the State.

26 10-1302.

27 (A) (1) SUBJECT TO PARAGRAPH (2) OF THIS SUBSECTION, THIS
28 SUBTITLE APPLIES ONLY TO THE COLLECTION, PROCESSING, AND SHARING OF
29 PERSONALLY IDENTIFIABLE INFORMATION BY A UNIT.

30 (2) THIS SUBTITLE DOES NOT APPLY TO THE COLLECTION,
31 PROCESSING, OR SHARING OF PERSONALLY IDENTIFIABLE INFORMATION
32 EXCLUSIVELY FOR PURPOSES OF:

- 1 **(I) PUBLIC HEALTH;**
2 **(II) PUBLIC SAFETY;**
3 **(III) STATE SECURITY;**
4 **(IV) STATE PERSONNEL OR RETIREMENT AND PENSION SYSTEM**
5 **MANAGEMENT; OR**
6 **(V) THE INVESTIGATION AND PROSECUTION OF CRIMINAL**
7 **OFFENSES.**

8 **[(a)] (B)** This subtitle does not apply to **[personal] PERSONALLY**
9 **IDENTIFIABLE** information that:

- 10 (1) is publicly available information that is lawfully made available to the
11 general public from federal, State, or local government records;
12 (2) an individual has consented to have publicly disseminated or listed;
13 (3) except for a medical record that a person is prohibited from redisclosing
14 under § 4-302(d) of the Health – General Article, is disclosed in accordance with the federal
15 Health Insurance Portability and Accountability Act; or
16 (4) is disclosed in accordance with the federal Family Educational Rights
17 and Privacy Act.

18 **[(b)] (C)** This subtitle does not apply to the Legislative or Judicial Branch of
19 State government **OR THE UNIVERSITY SYSTEM OF MARYLAND.**

20 **(D) THIS SUBTITLE MAY NOT BE CONSTRUED TO:**

- 21 **(1) ALTER OR SUPERSEDE THE REQUIREMENTS OF THE PUBLIC**
22 **INFORMATION ACT;**
23 **(2) AFFECT THE AUTHORITY OF A UNIT TO MAKE DETERMINATIONS**
24 **REGARDING THE DISCLOSURE OF PUBLIC RECORDS CONSISTENT WITH THE PUBLIC**
25 **INFORMATION ACT; OR**
26 **(3) REQUIRE A UNIT TO PROVIDE ACCESS TO PUBLIC RECORDS NOT**
27 **DISCLOSABLE UNDER THE PUBLIC INFORMATION ACT.**

28 **(E) THE SECRETARY OF INFORMATION TECHNOLOGY MAY ADOPT**
29 **REGULATIONS TO CARRY OUT THIS SUBTITLE.**

1 10-1303.

2 When a unit is destroying records of an individual that contain [personal]
3 **PERSONALLY IDENTIFIABLE** information of the individual, the unit shall take reasonable
4 steps to protect against unauthorized access to or use of the [personal] **PERSONALLY**
5 **IDENTIFIABLE** information, taking into account:

- 6 (1) the sensitivity of the records;
- 7 (2) the nature of the unit and its operations;
- 8 (3) the costs and benefits of different destruction methods; and
- 9 (4) available technology.

10 10-1304.

11 (a) **(1)** To protect [personal] **PERSONALLY IDENTIFIABLE** information from
12 unauthorized access, use, modification, or disclosure **AND SUBJECT TO PARAGRAPH (2)**
13 **OF THIS SUBSECTION**, a unit that collects [personal] **PERSONALLY IDENTIFIABLE**
14 information of an individual shall implement and maintain reasonable security procedures
15 and practices that are appropriate to the nature of the [personal] **PERSONALLY**
16 **IDENTIFIABLE** information collected and the nature of the unit and its operations.

17 **(2) (I) THIS PARAGRAPH DOES NOT APPLY TO:**

- 18 1. **THE OFFICE OF THE ATTORNEY GENERAL; OR**
- 19 2. **A UNIT DESCRIBED IN § 10-1301(G)(2) OF THIS**
20 **SUBTITLE.**

21 **(II) EACH UNIT SHALL COMPLY WITH STANDARDS AND**
22 **GUIDELINES, INCLUDING FEDERAL INFORMATION PROCESSING STANDARDS**
23 **(FIPS) 199, FIPS 200, AND THE NATIONAL INSTITUTE OF STANDARDS AND**
24 **TECHNOLOGY (NIST) SPECIAL PUBLICATION (SP) 800 SERIES, TO ENSURE THAT**
25 **THE SECURITY OF ALL INFORMATION SYSTEMS AND APPLICATIONS IS MANAGED**
26 **THROUGH THE NIST RISK MANAGEMENT FRAMEWORK, WHICH REQUIRES THAT:**

- 27 1. **THE SYSTEM IS CATEGORIZED BASED ON A FIPS 199**
28 **ANALYSIS;**
- 29 2. **THE SECURITY CONTROLS ARE SELECTED BASED ON**
30 **THE SECURITY CATEGORIZATION OF THE SYSTEM;**
- 31 3. **THE CONTROLS ARE IMPLEMENTED WITHIN THE**

1 INFORMATION SYSTEM OR APPLICATION;

2 4. THE CONTROLS ARE ASSESSED BY A
3 THIRD-PARTY ASSESSOR;

4 5. THE SYSTEM IS AUTHORIZED TO OPERATE BY AN
5 AUTHORIZING OFFICIAL WHO REVIEWS THE SECURITY AUTHORIZATION PACKAGE
6 AND ACCEPTS THE RISKS IDENTIFIED;

7 6. THE IMPLEMENTED SECURITY CONTROLS ARE
8 CONTINUOUSLY MONITORED FOR EFFECTIVENESS; AND

9 7. THE REASSESSMENT AND AUTHORIZATION OF
10 SYSTEMS ARE TO BE COMPLETED ON AN ANNUAL BASIS.

11 (b) (1) This subsection shall apply to a written contract or agreement that is
12 entered into on or after July 1, 2014.

13 (2) A unit that uses a nonaffiliated third party as a service provider to
14 perform services for the unit and discloses [personal] PERSONALLY IDENTIFIABLE
15 information about an individual under a written contract or agreement with the third party
16 shall require by written contract or agreement that the third party implement and
17 maintain reasonable security procedures and practices that:

18 (i) are appropriate to the nature of the [personal] PERSONALLY
19 IDENTIFIABLE information disclosed to the nonaffiliated third party; and

20 (ii) are reasonably designed to help protect the [personal]
21 PERSONALLY IDENTIFIABLE information from unauthorized access, use, modification,
22 disclosure, or destruction.

23 (C) (1) EACH UNIT SHALL UNDERTAKE ACTIVITIES COMPRISING THE
24 COLLECTION, PROCESSING, AND SHARING OF PERSONALLY IDENTIFIABLE
25 INFORMATION IN GOOD FAITH.

26 (2) (I) THIS PARAGRAPH DOES NOT APPLY TO:

27 1. THE OFFICE OF THE ATTORNEY GENERAL; OR

28 2. A UNIT DESCRIBED IN § 10-1301(G)(2) OF THIS
29 SUBTITLE.

30 (II) EACH UNIT SHALL:

31 1. IDENTIFY AND DOCUMENT THE LEGAL AUTHORITY

1 FOR THE UNIT'S COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION;

2 2. DESCRIBE THE PURPOSE OF THE PERSONALLY
3 IDENTIFIABLE INFORMATION COLLECTION AND PROVIDE NOTICE OF THE
4 PERSONALLY IDENTIFIABLE INFORMATION COLLECTION TO THE INDIVIDUAL AT
5 THE TIME OF COLLECTION AND IN A PRIVACY NOTICE PROMINENTLY DISPLAYED ON
6 THE UNIT'S WEBSITE;

7 3. ADOPT A PRIVACY GOVERNANCE AND RISK
8 MANAGEMENT PROGRAM AND IMPLEMENT REASONABLE SECURITY PROCEDURES
9 AND PRACTICES, CONSISTENT WITH POLICIES AND STANDARDS ESTABLISHED BY
10 THE DEPARTMENT OF INFORMATION TECHNOLOGY, TO ENSURE THAT
11 CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF ALL PERSONALLY
12 IDENTIFIABLE INFORMATION ARE MAINTAINED;

13 4. ESTABLISH PRIVACY REQUIREMENTS APPLICABLE TO
14 CONTRACTORS, SERVICE PROVIDERS, AND OTHER THIRD PARTIES AND
15 INCORPORATE THE REQUIREMENTS INTO AGREEMENTS ENTERED INTO WITH THE
16 THIRD PARTIES;

17 5. TAKE REASONABLE STEPS TO ENSURE THAT
18 PERSONALLY IDENTIFIABLE INFORMATION COLLECTED IS ACCURATE, RELEVANT,
19 TIMELY, AND COMPLETE;

20 6. TAKE REASONABLE STEPS TO IMPLEMENT MEANS TO
21 LIMIT THE PERSONALLY IDENTIFIABLE INFORMATION COLLECTED TO
22 INFORMATION RELEVANT AND NECESSARY TO ADDRESS THE LEGALLY AUTHORIZED
23 PURPOSE OF THE COLLECTION;

24 7. IMPLEMENT PROCESSES TO PROVIDE AN INDIVIDUAL
25 ACCESS TO THE INDIVIDUAL'S PERSONALLY IDENTIFIABLE INFORMATION AND TO
26 ALLOW THE INDIVIDUAL TO CORRECT OR AMEND THE PERSONALLY IDENTIFIABLE
27 INFORMATION PROCESSED BY THE UNIT; AND

28 8. SUBJECT TO SUBSECTION (D) OF THIS SECTION,
29 ESTABLISH CLEAR AND COMPREHENSIVE NOTICE PROVISIONS TO INFORM THE
30 PUBLIC AND INDIVIDUALS OF UNIT PRACTICES AND ACTIVITIES REGARDING THE
31 USE OF PERSONALLY IDENTIFIABLE INFORMATION.

32 (D) (1) THIS SUBSECTION DOES NOT APPLY TO:

33 (I) THE OFFICE OF THE ATTORNEY GENERAL; OR

34 (II) A UNIT DESCRIBED IN § 10-1301(G)(2) OF THIS SUBTITLE.

1 **(2) EACH UNIT SHALL:**

2 **(I) ADVISE AN INDIVIDUAL REQUESTED TO PROVIDE**
3 **PERSONALLY IDENTIFIABLE INFORMATION WHETHER:**

4 **1. THE PERSONALLY IDENTIFIABLE INFORMATION**
5 **REQUESTED IS REQUIRED TO BE PROVIDED BY LAW; OR**

6 **2. THE PROVISION OF THE PERSONALLY IDENTIFIABLE**
7 **INFORMATION REQUESTED IS VOLUNTARY AND SUBJECT TO THE INDIVIDUAL'S**
8 **DISCRETION TO REFUSE TO PROVIDE THE PERSONALLY IDENTIFIABLE**
9 **INFORMATION;**

10 **(II) PROVIDE AN INDIVIDUAL WITH CLEAR AND CONSPICUOUS**
11 **MEANS TO ACCESS:**

12 **1. THE TYPES OF PERSONALLY IDENTIFIABLE**
13 **INFORMATION COLLECTED ABOUT THE INDIVIDUAL;**

14 **2. THE TYPES OF SOURCES FROM WHICH THE**
15 **PERSONALLY IDENTIFIABLE INFORMATION WAS COLLECTED;**

16 **3. THE PURPOSE FOR COLLECTING THE PERSONALLY**
17 **IDENTIFIABLE INFORMATION;**

18 **4. THE THIRD PARTIES WITH WHOM THE PERSONALLY**
19 **IDENTIFIABLE INFORMATION IS SHARED; AND**

20 **5. THE SPECIFIC PERSONALLY IDENTIFIABLE**
21 **INFORMATION COLLECTED ABOUT THE INDIVIDUAL;**

22 **(III) INCLUDE THE MEANS PROVIDED UNDER ITEM (II) OF THIS**
23 **PARAGRAPH IN THE NOTICES PROVIDED TO THE INDIVIDUAL REGARDING THE**
24 **COLLECTION, PROCESSING, AND SHARING OF THE INDIVIDUAL'S PERSONALLY**
25 **IDENTIFIABLE INFORMATION;**

26 **(IV) AT OR BEFORE THE POINT OF SHARING PERSONALLY**
27 **IDENTIFIABLE INFORMATION, PROVIDE NOTICE TO AN INDIVIDUAL OF THE UNIT'S**
28 **SHARING OF THE INDIVIDUAL'S PERSONALLY IDENTIFIABLE INFORMATION,**
29 **INCLUDING:**

30 **1. THE NATURE AND SOURCES OF INFORMATION**
31 **SHARED;**

1 2. THE PURPOSE FOR WHICH THE INFORMATION IS
2 SHARED;

3 3. THE RECIPIENTS OF THE SHARED INFORMATION;

4 4. THE AUTHORITY UNDER WHICH THE INFORMATION IS
5 SHARED;

6 5. ANY RIGHTS THE INDIVIDUAL HAS TO DECLINE THE
7 UNIT'S SHARING OF PERSONALLY IDENTIFIABLE INFORMATION; AND

8 6. THE INDIVIDUAL'S RIGHT AND MEANS TO OBTAIN AND
9 REVIEW THE PERSONALLY IDENTIFIABLE INFORMATION SHARED BY THE UNIT;

10 (V) PROVIDE AN INDIVIDUAL WITH A PROCESS TO DELETE OR
11 CORRECT PERSONALLY IDENTIFIABLE INFORMATION SHARED WITH THIRD PARTIES
12 IF THE SHARING OF THE INFORMATION IS NOT REQUIRED BY LAW; AND

13 (VI) PROVIDE AN INDIVIDUAL WITH THE MEANS TO OPT OUT OF
14 SHARING INFORMATION WITH THIRD PARTIES IF THE SHARING OF THE
15 INFORMATION IS NOT REQUIRED BY LAW.

16 10-1305.

17 (a) (1) In this section, "breach of the security of a system" means the
18 unauthorized acquisition of computerized data that compromises the security,
19 confidentiality, or integrity of the [personal] **PERSONALLY IDENTIFIABLE** information
20 maintained by a unit.

21 (2) "Breach of the security of a system" does not include the good faith
22 acquisition of [personal] **PERSONALLY IDENTIFIABLE** information by an employee or
23 agent of a unit for the purposes of the unit, provided that the [personal] **PERSONALLY**
24 **IDENTIFIABLE** information is not used or subject to further unauthorized disclosure.

25 (b) (1) If a unit that collects computerized data that includes [personal]
26 **PERSONALLY IDENTIFIABLE** information of an individual discovers or is notified of a
27 breach of the security of a system, the unit shall conduct in good faith a reasonable and
28 prompt investigation to determine whether the unauthorized acquisition of [personal]
29 **PERSONALLY IDENTIFIABLE** information of the individual has resulted in or is likely to
30 result in the misuse of the information.

31 (2) (i) Except as provided in subparagraph (ii) of this paragraph, if after
32 the investigation is concluded, the unit determines that the misuse of the individual's
33 [personal] **PERSONALLY IDENTIFIABLE** information has occurred or is likely to occur, the

1 unit or the nonaffiliated third party, if authorized under a written contract or agreement
2 with the unit, shall notify the individual of the breach.

3 (ii) Unless the unit or nonaffiliated third party knows that the
4 encryption key has been broken, a unit or the nonaffiliated third party is not required to
5 notify an individual under subparagraph (i) of this paragraph if:

6 1. the [personal] **PERSONALLY IDENTIFIABLE** information
7 of the individual was secured by encryption or redacted; and

8 2. the encryption key has not been compromised or disclosed.

9 (c) (1) A nonaffiliated third party that maintains computerized data that
10 includes [personal] **PERSONALLY IDENTIFIABLE** information provided by a unit shall
11 notify the unit of a breach of the security of a system if the unauthorized acquisition of the
12 individual's [personal] **PERSONALLY IDENTIFIABLE** information has occurred or is likely
13 to occur.

14 (g) The notification required under subsection (b) of this section shall include:

15 (1) to the extent possible, a description of the categories of information that
16 were, or are reasonably believed to have been, acquired by an unauthorized person,
17 including which of the elements of [personal] **PERSONALLY IDENTIFIABLE** information
18 were, or are reasonably believed to have been, acquired;

19 (h) (2) In addition to the notice required under paragraph (1) of this
20 subsection, a unit, as defined in [§ 10–1301(f)(1)] **§ 10–1301(G)(1)** of this subtitle, shall
21 provide notice of a breach of security to the Department of Information Technology.

22 (j) Compliance with this section does not relieve a unit from a duty to comply
23 with any other requirements of federal law relating to the protection and privacy of
24 [personal] **PERSONALLY IDENTIFIABLE** information.

25 SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect
26 October 1, 2020.