

HOUSE BILL 340

P1

0lr0174
CF SB 274

By: **The Speaker (By Request – Administration) and Delegates Adams, Anderton, Arentz, Arian, Beitzel, Chisholm, Ciliberti, Clark, Corderman, Ghrist, Grammer, Griffith, Hartman, Howard, Jacobs, Kipke, Kittleman, Krebs, Long, Malone, Mautz, McComas, McKay, Metzgar, Morgan, Otto, Reilly, Rose, Saab, Szeliga, ~~and Wivell~~ Wivell, Bagnall, Barron, Belcastro, Bhandari, Charles, Cullison, Hill, Johnson, Kelly, Kerr, R. Lewis, Pena-Melnyk, Pendergrass, Rosenberg, and K. Young**

Introduced and read first time: January 20, 2020

Assigned to: Health and Government Operations

Committee Report: Favorable with amendments

House action: Adopted

Read second time: March 10, 2020

CHAPTER _____

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

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 units to provide an individual with a certain process and the means to opt out of
 2 sharing information with third parties under certain circumstances; authorizing the
 3 Secretary of Information Technology to adopt certain regulations; establishing that
 4 certain provisions of law do not apply to ~~the University System of Maryland~~ public
 5 institutions of higher education; providing for the application and construction of
 6 certain provisions of law; providing that certain provisions of this Act do not apply
 7 to the Office of the Attorney General; defining certain terms; repealing certain
 8 definitions; making conforming changes; requiring each public institution of higher
 9 education to submit a certain report to the Governor on or before certain dates each
 10 year; providing for the termination of certain provisions of this Act; and generally
 11 relating to the protection of personally identifiable information by government
 12 agencies.

13 BY repealing and reenacting, with amendments,

14 Article – State Government

15 Section 10–1301 through 10–1304 and 10–1305(a), (b)(1) and (2), (c)(1), (g)(1), (h)(2),
 16 and (j)

17 Annotated Code of Maryland

18 (2014 Replacement Volume and 2019 Supplement)

19 SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND,

20 That the Laws of Maryland read as follows:

21 **Article – State Government**

22 10–1301.

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

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

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

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

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

34 (i) a Social Security number;

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

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

3 (iv) an Individual Taxpayer Identification Number; or

4 (v) a financial or other account number, a credit card number, or a
5 debit card number that, in combination with any required security code, access code, or
6 password, would permit access to an individual's account.

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

8 (d) "Reasonable security procedures and practices" means data security
9 procedures and practices developed, in good faith, and set forth in a written information
10 security policy.]

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

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

16 (I) UNIQUE PERSONAL IDENTIFIERS, INCLUDING:

17 1. A FULL NAME;

18 2. A FIRST INITIAL AND LAST NAME;

19 3. A SOCIAL SECURITY NUMBER;

20 4. A DRIVER'S LICENSE NUMBER, A STATE
21 IDENTIFICATION NUMBER, OR ANY OTHER IDENTIFICATION NUMBER ISSUED BY A
22 UNIT; AND

23 5. A PASSPORT NUMBER;

24 (II) CHARACTERISTICS OF CLASSIFICATIONS PROTECTED
25 UNDER FEDERAL OR STATE LAW;

26 (III) BIOMETRIC INFORMATION INCLUDING AN INDIVIDUAL'S
27 PHYSIOLOGICAL, BIOLOGICAL, OR BEHAVIORAL CHARACTERISTICS, INCLUDING AN
28 INDIVIDUAL'S DEOXYRIBONUCLEIC ACID (DNA), THAT CAN BE USED, SINGLY OR IN
29 COMBINATION WITH EACH OTHER OR WITH OTHER IDENTIFYING DATA, TO
30 ESTABLISH INDIVIDUAL IDENTITY;

1 (IV) GEOLOCATION DATA;

2 (V) INTERNET OR OTHER ELECTRONIC NETWORK ACTIVITY
3 INFORMATION, INCLUDING BROWSING HISTORY, SEARCH HISTORY, AND
4 INFORMATION REGARDING AN INDIVIDUAL'S INTERACTION WITH AN INTERNET
5 WEBSITE, APPLICATION, OR ADVERTISEMENT;

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

9 (VII) A FINANCIAL OR OTHER ACCOUNT NUMBER, A CREDIT CARD
10 NUMBER, OR A DEBIT CARD NUMBER THAT, IN COMBINATION WITH ANY REQUIRED
11 SECURITY CODE, ACCESS CODE, OR PASSWORD, WOULD PERMIT ACCESS TO AN
12 INDIVIDUAL'S ACCOUNT.

13 (2) "PERSONALLY IDENTIFIABLE INFORMATION" DOES NOT
14 INCLUDE:

15 (I) VOTER REGISTRATION INFORMATION;

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

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

21 (E) "REASONABLE SECURITY PROCEDURES AND PRACTICES" MEANS
22 SECURITY PROTECTIONS THAT ALIGN WITH DEPARTMENT OF INFORMATION
23 TECHNOLOGY POLICIES AND THE FEDERAL INFORMATION SECURITY
24 MODERNIZATION ACT (FISMA) OF 2014.

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

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

28 (1) an executive agency, or a department, a board, a commission, an
29 authority, ~~a public institution of higher education,~~ a unit or an instrumentality of the State;
30 or

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

10-1302.

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

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

(I) PUBLIC HEALTH;

(II) PUBLIC SAFETY;

(III) STATE SECURITY;

(IV) STATE PERSONNEL OR RETIREMENT AND PENSION SYSTEM MANAGEMENT; OR

(V) THE INVESTIGATION AND PROSECUTION OF CRIMINAL OFFENSES.

(3) THIS SUBTITLE DOES NOT APPLY TO THE SHARING OF PERSONALLY IDENTIFIABLE INFORMATION BETWEEN THE MARYLAND DEPARTMENT OF HEALTH AND ANY STATE OR FEDERAL AGENCY AS ALLOWED BY LAW OR REGULATION.

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

(1) is publicly available information that is lawfully made available to the general public from federal, State, or local government records;

(2) an individual has consented to have publicly disseminated or listed;

(3) except for a medical record that a person is prohibited from redisclosing under § 4-302(d) of the Health – General Article, is disclosed in accordance with the federal Health Insurance Portability and Accountability Act; or

(4) is disclosed in accordance with the federal Family Educational Rights and Privacy Act.

1 **[(b)] (C)** This subtitle does not apply to the Legislative or Judicial Branch of
 2 State government **OR ~~THE UNIVERSITY SYSTEM OF MARYLAND~~ A PUBLIC**
 3 **INSTITUTION OF HIGHER EDUCATION.**

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

5 **(1) ALTER OR SUPERSEDE THE REQUIREMENTS OF THE PUBLIC**
 6 **INFORMATION ACT;**

7 **(2) AFFECT THE AUTHORITY OF A UNIT TO MAKE DETERMINATIONS**
 8 **REGARDING THE DISCLOSURE OF PUBLIC RECORDS CONSISTENT WITH THE PUBLIC**
 9 **INFORMATION ACT; OR**

10 **(3) REQUIRE A UNIT TO PROVIDE ACCESS TO PUBLIC RECORDS NOT**
 11 **DISCLOSABLE UNDER THE PUBLIC INFORMATION ACT.**

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

14 10-1303.

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

19 (1) the sensitivity of the records;

20 (2) the nature of the unit and its operations;

21 (3) the costs and benefits of different destruction methods; and

22 (4) available technology.

23 10-1304.

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

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

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

3 SUBTITLE.

4 ~~(H) EACH UNIT SHALL COMPLY WITH STANDARDS AND~~
5 ~~GUIDELINES, INCLUDING FEDERAL INFORMATION PROCESSING STANDARDS~~
6 ~~(FIPS) 199, FIPS 200, AND THE NATIONAL INSTITUTE OF STANDARDS AND~~
7 ~~TECHNOLOGY (NIST) SPECIAL PUBLICATION (SP) 800 SERIES, TO ENSURE THAT~~
8 ~~THE SECURITY OF ALL INFORMATION SYSTEMS AND APPLICATIONS IS MANAGED~~
9 ~~THROUGH THE NIST RISK MANAGEMENT FRAMEWORK, WHICH REQUIRES THAT:~~

10 ~~1. THE SYSTEM IS CATEGORIZED BASED ON A FIPS 199~~
11 ~~ANALYSIS;~~

12 (II) EACH UNIT SHALL COMPLY WITH STANDARDS AND
13 GUIDELINES ESTABLISHED BY THE DEPARTMENT OF INFORMATION TECHNOLOGY,
14 TO ENSURE THAT THE SECURITY OF ALL INFORMATION SYSTEMS AND APPLICATIONS
15 IS MANAGED THROUGH STATE-SPECIFIED RISK MANAGEMENT FRAMEWORK, WHICH
16 REQUIRES THAT:

17 1. THE SYSTEM IS CATEGORIZED BASED ON AN ANALYSIS
18 OF THE STATE SYSTEM CATEGORIZATION CRITERIA;

19 2. THE SECURITY CONTROLS ARE SELECTED BASED ON
20 THE SECURITY CATEGORIZATION OF THE SYSTEM;

21 3. THE CONTROLS ARE IMPLEMENTED WITHIN THE
22 INFORMATION SYSTEM OR APPLICATION;

23 4. THE CONTROLS ARE ASSESSED BY A
24 THIRD-PARTY ASSESSOR;

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

28 6. THE IMPLEMENTED SECURITY CONTROLS ARE
29 CONTINUOUSLY MONITORED FOR EFFECTIVENESS; AND

30 7. THE REASSESSMENT AND AUTHORIZATION OF
31 SYSTEMS ARE TO BE COMPLETED ~~ON AN ANNUAL BASIS~~ NOT LESS THAN ONCE EVERY
32 3 YEARS.

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

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

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

10 (ii) are reasonably designed to help protect the [personal]
11 **PERSONALLY IDENTIFIABLE** information from unauthorized access, use, modification,
12 disclosure, or destruction.

13 (c) (1) **EACH UNIT SHALL UNDERTAKE ACTIVITIES COMPRISING THE**
14 **COLLECTION, PROCESSING, AND SHARING OF PERSONALLY IDENTIFIABLE**
15 **INFORMATION IN GOOD FAITH.**

16 (2) (i) **THIS PARAGRAPH DOES NOT APPLY TO:**

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

20 (ii) **EACH UNIT SHALL:**

21 1. **IDENTIFY AND DOCUMENT THE LEGAL AUTHORITY**
22 **FOR THE UNIT'S COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION;**

23 2. **DESCRIBE THE PURPOSE OF THE PERSONALLY**
24 **IDENTIFIABLE INFORMATION COLLECTION AND PROVIDE NOTICE OF THE**
25 **PERSONALLY IDENTIFIABLE INFORMATION COLLECTION TO THE INDIVIDUAL AT**
26 **THE TIME OF COLLECTION AND IN A PRIVACY NOTICE PROMINENTLY DISPLAYED ON**
27 **THE UNIT'S WEBSITE;**

28 3. **ADOPT A PRIVACY GOVERNANCE AND RISK**
29 **MANAGEMENT PROGRAM AND IMPLEMENT REASONABLE SECURITY PROCEDURES**
30 **AND PRACTICES, CONSISTENT WITH POLICIES AND STANDARDS ESTABLISHED BY**
31 **THE DEPARTMENT OF INFORMATION TECHNOLOGY, TO ENSURE THAT**
32 **CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF ALL PERSONALLY**
33 **IDENTIFIABLE INFORMATION ARE MAINTAINED;**

1 4. ESTABLISH PRIVACY REQUIREMENTS APPLICABLE TO
2 CONTRACTORS, SERVICE PROVIDERS, AND OTHER THIRD PARTIES AND
3 INCORPORATE THE REQUIREMENTS INTO AGREEMENTS ENTERED INTO WITH THE
4 THIRD PARTIES;

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

8 6. TAKE REASONABLE STEPS TO IMPLEMENT MEANS TO
9 LIMIT THE PERSONALLY IDENTIFIABLE INFORMATION COLLECTED TO
10 INFORMATION RELEVANT AND NECESSARY TO ADDRESS THE LEGALLY AUTHORIZED
11 PURPOSE OF THE COLLECTION;

12 7. IMPLEMENT PROCESSES TO PROVIDE AN INDIVIDUAL
13 ACCESS TO THE INDIVIDUAL'S PERSONALLY IDENTIFIABLE INFORMATION AND TO
14 ALLOW THE INDIVIDUAL TO CORRECT OR AMEND THE PERSONALLY IDENTIFIABLE
15 INFORMATION PROCESSED BY THE UNIT; AND

16 8. SUBJECT TO SUBSECTION (D) OF THIS SECTION,
17 ESTABLISH CLEAR AND COMPREHENSIVE NOTICE PROVISIONS TO INFORM THE
18 PUBLIC AND INDIVIDUALS OF UNIT PRACTICES AND ACTIVITIES REGARDING THE
19 USE OF PERSONALLY IDENTIFIABLE INFORMATION.

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

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

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

23 (2) EACH UNIT SHALL:

24 (I) ADVISE AN INDIVIDUAL REQUESTED TO PROVIDE
25 PERSONALLY IDENTIFIABLE INFORMATION WHETHER:

26 1. THE PERSONALLY IDENTIFIABLE INFORMATION
27 REQUESTED IS REQUIRED TO BE PROVIDED BY LAW; OR

28 2. THE PROVISION OF THE PERSONALLY IDENTIFIABLE
29 INFORMATION REQUESTED IS VOLUNTARY AND SUBJECT TO THE INDIVIDUAL'S
30 DISCRETION TO REFUSE TO PROVIDE THE PERSONALLY IDENTIFIABLE
31 INFORMATION;

1 **(II) PROVIDE AN INDIVIDUAL WITH CLEAR AND CONSPICUOUS**
2 **MEANS TO ACCESS:**

3 **1. THE TYPES OF PERSONALLY IDENTIFIABLE**
4 **INFORMATION COLLECTED ABOUT THE INDIVIDUAL;**

5 **2. THE TYPES OF SOURCES FROM WHICH THE**
6 **PERSONALLY IDENTIFIABLE INFORMATION WAS COLLECTED;**

7 **3. THE PURPOSE FOR COLLECTING THE PERSONALLY**
8 **IDENTIFIABLE INFORMATION;**

9 **4. THE THIRD PARTIES WITH WHOM THE PERSONALLY**
10 **IDENTIFIABLE INFORMATION IS SHARED; AND**

11 **5. THE SPECIFIC PERSONALLY IDENTIFIABLE**
12 **INFORMATION COLLECTED ABOUT THE INDIVIDUAL;**

13 **(III) INCLUDE THE MEANS PROVIDED UNDER ITEM (II) OF THIS**
14 **PARAGRAPH IN THE NOTICES PROVIDED TO THE INDIVIDUAL REGARDING THE**
15 **COLLECTION, PROCESSING, AND SHARING OF THE INDIVIDUAL'S PERSONALLY**
16 **IDENTIFIABLE INFORMATION;**

17 **(IV) AT OR BEFORE THE POINT OF SHARING PERSONALLY**
18 **IDENTIFIABLE INFORMATION, PROVIDE NOTICE TO AN INDIVIDUAL OF THE UNIT'S**
19 **SHARING OF THE INDIVIDUAL'S PERSONALLY IDENTIFIABLE INFORMATION,**
20 **INCLUDING:**

21 **1. THE NATURE AND SOURCES OF INFORMATION**
22 **SHARED;**

23 **2. THE PURPOSE FOR WHICH THE INFORMATION IS**
24 **SHARED;**

25 **3. THE RECIPIENTS OF THE SHARED INFORMATION;**

26 **4. THE AUTHORITY UNDER WHICH THE INFORMATION IS**
27 **SHARED;**

28 **5. ANY RIGHTS THE INDIVIDUAL HAS TO DECLINE THE**
29 **UNIT'S SHARING OF PERSONALLY IDENTIFIABLE INFORMATION; AND**

30 **6. THE INDIVIDUAL'S RIGHT AND MEANS TO OBTAIN AND**
31 **REVIEW THE PERSONALLY IDENTIFIABLE INFORMATION SHARED BY THE UNIT;**

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

4 **(VI) PROVIDE AN INDIVIDUAL WITH THE MEANS TO OPT OUT OF**
5 **SHARING INFORMATION WITH THIRD PARTIES IF THE SHARING OF THE**
6 **INFORMATION IS NOT REQUIRED BY LAW.**

7 10–1305.

8 (a) (1) In this section, “breach of the security of a system” means the
9 unauthorized acquisition of computerized data that compromises the security,
10 confidentiality, or integrity of the [personal] **PERSONALLY IDENTIFIABLE** information
11 maintained by a unit.

12 (2) “Breach of the security of a system” does not include the good faith
13 acquisition of [personal] **PERSONALLY IDENTIFIABLE** information by an employee or
14 agent of a unit for the purposes of the unit, provided that the [personal] **PERSONALLY**
15 **IDENTIFIABLE** information is not used or subject to further unauthorized disclosure.

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

22 (2) (i) Except as provided in subparagraph (ii) of this paragraph, if after
23 the investigation is concluded, the unit determines that the misuse of the individual’s
24 [personal] **PERSONALLY IDENTIFIABLE** information has occurred or is likely to occur, the
25 unit or the nonaffiliated third party, if authorized under a written contract or agreement
26 with the unit, shall notify the individual of the breach.

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

- 30 1. the [personal] **PERSONALLY IDENTIFIABLE** information
31 of the individual was secured by encryption or redacted; and
- 32 2. the encryption key has not been compromised or disclosed.

33 (c) (1) A nonaffiliated third party that maintains computerized data that
34 includes [personal] **PERSONALLY IDENTIFIABLE** information provided by a unit shall
35 notify the unit of a breach of the security of a system if the unauthorized acquisition of the

1 individual's [personal] PERSONALLY IDENTIFIABLE information has occurred or is likely
2 to occur.

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

4 (1) to the extent possible, a description of the categories of information that
5 were, or are reasonably believed to have been, acquired by an unauthorized person,
6 including which of the elements of [personal] PERSONALLY IDENTIFIABLE information
7 were, or are reasonably believed to have been, acquired;

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

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

14 SECTION 2. AND BE IT FURTHER ENACTED, That, on or before December 1,
15 2020, and each year thereafter, each public institution of higher education shall submit a
16 report to the Governor that includes:

17 (1) a summary of the status of the implementation of any data privacy
18 framework;

19 (2) a description of any barriers or defects to implementation and solutions;

20 (3) the number and disposition of reported breaches, if any; and

21 (4) updates to project cost estimates.

22 SECTION ~~2~~ 3. AND BE IT FURTHER ENACTED, That this Act shall take effect
23 October 1, 2020. Section 2 of this Act shall remain effective for a period of 4 years and 2
24 months and, at the end of December 31, 2024, Section 2 of this Act, with no further action
25 required by the General Assembly, shall be abrogated and of no further force and effect.