HOUSE BILL 716

P1 9lr0130

By: **Chair, Health and Government Operations Committee (By Request – Departmental – Information Technology)**
Introduced and read first time: February 7, 2019
Assigned to: Health and Government Operations

A BILL ENTITLED

AN ACT concerning

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

FOR the purpose of requiring certain units of State government to comply with certain standards and guidelines to ensure that the security of all information systems and applications are managed through a certain framework; requiring certain units of State government to undertake activities comprising collection, processing, and sharing of personally identifiable information in good faith and in accordance with a certain provision of this Act; requiring the units to identify and document certain legal authority, describe a certain purpose and make certain notifications, adopt a certain privacy governance and risk management program, implement certain security measures, establish certain privacy requirements and incorporate the requirements into certain agreements, take certain steps, implement certain processes, and establish certain notice provisions; requiring the units to advise certain individuals whether certain information is required to be provided by law or whether the provision is voluntary and subject to certain discretion; requiring the units to provide an individual with certain means to access certain information and certain third parties; requiring the units to include certain means in certain notices and provide certain notices to individuals at or before the point of sharing personally identifiable information; requiring the units to provide an individual with a certain process and the means to opt out of sharing information with third parties under certain circumstances; providing for the application of certain provisions of law; defining certain terms; repealing certain definitions; making conforming changes; and generally relating to the protection of personally identifiable information by government agencies.

BY repealing and reenacting, with amendments,
Article – State Government
Section 10–1301 through 10–1304 and 10–1305(a), (b)(1) and (2), (c)(1), (g)(1), (h)(2), and (j)

EXPLANATION: **CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.**
[Brackets**]** indicate matter deleted from existing law.

Annotated Code of Maryland
(2014 Replacement Volume and 2018 Supplement)

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

Article – State Government

10–1301.

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

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

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

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

[(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;

(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) 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.

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

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

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

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

(I) UNIQUE PERSONAL IDENTIFIERS, INCLUDING:

1. A FULL NAME;

2. A FIRST INITIAL AND LAST NAME;

3. A SOCIAL SECURITY NUMBER;

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

5. A PASSPORT NUMBER;

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

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

(IV) GEOLOCATION DATA;

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

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

(VII) 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.

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

(I) VOTER REGISTRATION INFORMATION;

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

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

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

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

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

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

(IV) THE INVESTIGATION AND PROSECUTION OF CRIMINAL OFFENSES.

[(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.

[(b)**] (C)** This subtitle does not apply to the Legislative or Judicial Branch of State government.

10–1303.

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

(1) the sensitivity of the records;

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

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

(4) available technology.

10–1304.

(a) **(1)** To protect **[**personal**]** **PERSONALLY IDENTIFIABLE** information from unauthorized access, use, modification, or disclosure **AND SUBJECT TO PARAGRAPH (2) OF THIS SUBSECTION**, a unit that collects **[**personal**]** **PERSONALLY IDENTIFIABLE** information of an individual shall implement and maintain reasonable security procedures

and practices that are appropriate to the nature of the **[**personal**]** **PERSONALLY IDENTIFIABLE** information collected and the nature of the unit and its operations.

(2) THE UNIT SHALL COMPLY WITH STANDARDS AND GUIDELINES, INCLUDING FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) 199, FIPS 200, AND THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) SPECIAL PUBLICATION (SP) 800 SERIES, TO ENSURE THAT THE SECURITY OF ALL INFORMATION SYSTEMS AND APPLICATIONS IS MANAGED THROUGH THE RISK MANAGEMENT FRAMEWORK DEFINED IN NIST SP 800–37 REV 1, WHICH REQUIRES THAT:

(I) THE SYSTEM IS CATEGORIZED BASED ON A FIPS 199 ANALYSIS;

(II) THE SECURITY CONTROLS ARE SELECTED BASED ON THE SECURITY CATEGORIZATION OF THE SYSTEM;

(III) THE CONTROLS ARE IMPLEMENTED WITHIN THE INFORMATION SYSTEM OR APPLICATION;

(IV) THE CONTROLS ARE ASSESSED BY A THIRD–PARTY ASSESSOR;

(V) THE SYSTEM IS AUTHORIZED TO OPERATE BY AN AUTHORIZING OFFICIAL WHO REVIEWS THE SECURITY AUTHORIZATION PACKAGE AND ACCEPTS THE RISKS IDENTIFIED;

(VI) THE IMPLEMENTED SECURITY CONTROLS ARE CONTINUOUSLY MONITORED FOR EFFECTIVENESS; AND

(VII) THE REASSESSMENT AND AUTHORIZATION OF SYSTEMS ARE TO BE COMPLETED ON AN ANNUAL BASIS.

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

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

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

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

(C) (1) EACH UNIT SHALL UNDERTAKE ACTIVITIES COMPRISING THE COLLECTION, PROCESSING, AND SHARING OF PERSONALLY IDENTIFIABLE INFORMATION IN GOOD FAITH AND IN ACCORDANCE WITH THE REQUIREMENTS UNDER PARAGRAPH (2) OF THIS SUBSECTION.

(2) EACH UNIT SHALL:

(I) IDENTIFY AND DOCUMENT THE LEGAL AUTHORITY FOR THE UNIT'S COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION;

(II) DESCRIBE THE PURPOSE OF THE PERSONALLY IDENTIFIABLE INFORMATION COLLECTION AND PROVIDE NOTICE OF THE PERSONALLY IDENTIFIABLE INFORMATION COLLECTION TO THE INDIVIDUAL AT THE TIME OF COLLECTION AND IN A PRIVACY NOTICE PROMINENTLY DISPLAYED ON THE UNIT'S WEBSITE;

(III) ADOPT A PRIVACY GOVERNANCE AND RISK MANAGEMENT PROGRAM AND IMPLEMENT REASONABLE SECURITY PROCEDURES AND PRACTICES, CONSISTENT WITH POLICIES AND STANDARDS ESTABLISHED BY THE DEPARTMENT OF INFORMATION TECHNOLOGY, TO ENSURE THAT CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF ALL PERSONALLY IDENTIFIABLE INFORMATION IS MAINTAINED;

(IV) ESTABLISH PRIVACY REQUIREMENTS APPLICABLE TO CONTRACTORS, SERVICE PROVIDERS, AND OTHER THIRD PARTIES AND INCORPORATE THE REQUIREMENTS INTO AGREEMENTS ENTERED INTO WITH THE THIRD PARTIES;

(V) TAKE REASONABLE STEPS TO ENSURE THAT PERSONALLY IDENTIFIABLE INFORMATION COLLECTED IS ACCURATE, RELEVANT, TIMELY, AND COMPLETE;

(VI) TAKE REASONABLE STEPS TO IMPLEMENT MEANS TO MINIMIZE THE PERSONALLY IDENTIFIABLE INFORMATION COLLECTED TO INFORMATION RELEVANT AND NECESSARY TO ADDRESS THE LEGALLY AUTHORIZED PURPOSE OF THE COLLECTION;

(VII) IMPLEMENT PROCESSES TO PROVIDE AN INDIVIDUAL ACCESS TO THE INDIVIDUAL'S PERSONALLY IDENTIFIABLE INFORMATION AND TO

ALLOW THE INDIVIDUAL TO CORRECT OR AMEND THE PERSONALLY IDENTIFIABLE INFORMATION PROCESSED BY THE UNIT; AND

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

(D) EACH UNIT SHALL:

(1) ADVISE AN INDIVIDUAL REQUESTED TO PROVIDE PERSONALLY IDENTIFIABLE INFORMATION WHETHER:

(I) THE PERSONALLY IDENTIFIABLE INFORMATION REQUESTED IS REQUIRED TO BE PROVIDED BY LAW; OR

(II) THE PROVISION OF THE PERSONALLY IDENTIFIABLE INFORMATION REQUESTED IS VOLUNTARY AND SUBJECT TO THE INDIVIDUAL'S DISCRETION TO REFUSE TO PROVIDE THE PERSONALLY IDENTIFIABLE INFORMATION;

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

(I) THE TYPES OF PERSONALLY IDENTIFIABLE INFORMATION COLLECTED ABOUT THE INDIVIDUAL;

(II) THE TYPES OF SOURCES FROM WHICH THE PERSONALLY IDENTIFIABLE INFORMATION WAS COLLECTED;

(III) THE PURPOSE FOR COLLECTING THE PERSONALLY IDENTIFIABLE INFORMATION;

(IV) THE THIRD PARTIES WITH WHOM THE PERSONALLY IDENTIFIABLE INFORMATION IS SHARED; AND

(V) THE SPECIFIC PERSONALLY IDENTIFIABLE INFORMATION COLLECTED ABOUT THE INDIVIDUAL;

(3) INCLUDE THE MEANS PROVIDED UNDER ITEM (2) OF THIS SUBSECTION IN THE NOTICES PROVIDED TO THE INDIVIDUAL REGARDING THE COLLECTION, PROCESSING, AND SHARING OF THE INDIVIDUAL'S PERSONALLY IDENTIFIABLE INFORMATION;

(4) AT OR BEFORE THE POINT OF SHARING PERSONALLY IDENTIFIABLE INFORMATION, PROVIDE NOTICE TO AN INDIVIDUAL OF THE UNIT'S SHARING OF THE INDIVIDUAL'S PERSONALLY IDENTIFIABLE INFORMATION, INCLUDING:

(I) THE NATURE AND SOURCES OF INFORMATION SHARED;

(II) THE PURPOSE FOR WHICH THE INFORMATION IS SHARED;

(III) THE RECIPIENTS OF THE SHARED INFORMATION;

(IV) THE AUTHORITY UNDER WHICH THE INFORMATION IS SHARED;

(V) ANY RIGHTS THE INDIVIDUAL HAS TO DECLINE THE UNIT'S SHARING OF PERSONALLY IDENTIFIABLE INFORMATION; AND

(VI) THE INDIVIDUAL'S RIGHT AND MEANS TO OBTAIN AND REVIEW THE PERSONALLY IDENTIFIABLE INFORMATION SHARED BY THE UNIT;

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

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

10–1305.

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

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

(b) (1) If a unit that collects computerized data that includes **[**personal**]** **PERSONALLY IDENTIFIABLE** information of an individual discovers or is notified of a breach of the security of a system, the unit shall conduct in good faith a reasonable and

prompt investigation to determine whether the unauthorized acquisition of **[**personal**]** **PERSONALLY IDENTIFIABLE** information of the individual has resulted in or is likely to result in the misuse of the information.

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

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

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

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

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

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

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

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

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

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2019.