SENATE BILL 588

P1, F2 0lr2028
CF 0lr2299

By: **Senator Kagan**
Introduced and read first time: January 31, 2020
Assigned to: Education, Health, and Environmental Affairs

A BILL ENTITLED

AN ACT concerning

State Government – Protection of Personally Identifiable Information – University System of Maryland

FOR the purpose of excluding the University System of Maryland from certain provisions of law governing protection of information by government agencies; requiring the University System of Maryland to review and designate certain systems as systems of record based on certain criteria; requiring the University to develop and adopt a certain privacy governance program to govern each system of record; requiring the University to develop and adopt a certain information security and risk management program for the protection of personally identifiable information; requiring the University to publish a certain privacy notice on the University's website; requiring the notice to include certain information; requiring the University, when destroying certain records, to take certain steps to protect against unauthorized access to or use of personally identifiable information; requiring the University, if it discovers or is notified of a breach of the security of a system, to conduct a certain investigation and, if the University determines that a certain breach has occurred, provide certain notices to certain individuals in a certain manner; establishing that this Act does not apply to certain personally identifiable information; establishing that compliance with certain provisions of law does not authorize the University to fail to comply with certain other provisions of law; defining certain terms; altering a certain definition; providing for a delayed effective date; and generally relating to protection of personally identifiable information by the University System of Maryland.

BY repealing and reenacting, without amendments,
Article – State Government
Section 10–1301(a)
Annotated Code of Maryland
(2014 Replacement Volume and 2019 Supplement)

BY repealing and reenacting, with amendments,
Article – State Government

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

Section 10–1301(f)
Annotated Code of Maryland
(2014 Replacement Volume and 2019 Supplement)

BY adding to
Article – State Government
Section 10–13A–01 through 10–13A–04 to be under the new subtitle "Subtitle 13A. Protection of Personally Identifiable Information by the University System of Maryland"
Annotated Code of Maryland
(2014 Replacement Volume and 2019 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.

(f) **(1)** "Unit" means:

[(1)**]** **(I)** an executive agency, or a department, a board, a commission, an authority, a public institution of higher education **OTHER THAN THE UNIVERSITY SYSTEM OF MARYLAND**, a unit**,** or an instrumentality of the State; or

[(2)**]** **(II)** 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.

(2) "UNIT" DOES NOT INCLUDE THE UNIVERSITY SYSTEM OF MARYLAND.

SUBTITLE 13A. PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION BY THE UNIVERSITY SYSTEM OF MARYLAND.

10–13A–01.

(A) IN THIS SUBTITLE THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED.

(B) (1) "BREACH OF THE SECURITY OF A SYSTEM" MEANS THE UNAUTHORIZED ACQUISITION OF PERSONALLY IDENTIFIABLE INFORMATION MAINTAINED BY THE UNIVERSITY SYSTEM OF MARYLAND THAT CREATES A

REASONABLE RISK OF HARM TO THE INDIVIDUAL WHOSE PERSONALLY IDENTIFIABLE INFORMATION WAS SUBJECT TO UNAUTHORIZED ACQUISITION.

(2) "BREACH OF THE SECURITY OF A SYSTEM" DOES NOT INCLUDE:

(I) THE GOOD FAITH ACQUISITION OF PERSONALLY IDENTIFIABLE INFORMATION BY AN EMPLOYEE OR AGENT OF THE UNIVERSITY SYSTEM OF MARYLAND FOR THE PURPOSES OF THE UNIVERSITY, PROVIDED THAT THE PERSONALLY IDENTIFIABLE INFORMATION IS NOT USED OR SUBJECT TO FURTHER UNAUTHORIZED DISCLOSURE; OR

(II) PERSONALLY IDENTIFIABLE INFORMATION THAT WAS SECURED BY ENCRYPTION OR REDACTED AND FOR WHICH THE ENCRYPTION KEY HAS NOT BEEN COMPROMISED OR DISCLOSED.

(C) "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.

(D) "INDIVIDUAL" MEANS A NATURAL PERSON.

(E) "LEGITIMATE BASIS" MEANS THE UNIVERSITY SYSTEM OF MARYLAND HAS A CONTRACTUAL NEED, PUBLIC INTEREST PURPOSE, BUSINESS PURPOSE, OR LEGAL OBLIGATION FOR PROCESSING OR THAT THE INDIVIDUAL HAS CONSENTED TO THE UNIVERSITY'S PROCESSING OF THE INDIVIDUAL'S PERSONALLY IDENTIFIABLE INFORMATION.

(F) (1) "PERSONALLY IDENTIFIABLE INFORMATION" MEANS ANY INFORMATION THAT, TAKEN ALONE OR IN COMBINATION WITH OTHER INFORMATION, ENABLES THE IDENTIFICATION OF AN INDIVIDUAL, INCLUDING:

(I) A FULL NAME;

(II) A SOCIAL SECURITY NUMBER;

(III) A DRIVER'S LICENSE NUMBER, STATE IDENTIFICATION

CARD NUMBER, OR OTHER INDIVIDUAL IDENTIFICATION NUMBER;

(IV) A PASSPORT NUMBER;

(V) 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;

(VI) GEOLOCATION DATA;

(VII) 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; AND

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

(G) "PROCESSING" MEANS ANY OPERATION OR SET OF OPERATIONS THAT IS PERFORMED ON PERSONALLY IDENTIFIABLE INFORMATION OR ON A SET OF PERSONALLY IDENTIFIABLE INFORMATION, WHETHER OR NOT BY AUTOMATED MEANS, INCLUDING COLLECTION, RECORDING, ORGANIZATION, STRUCTURING, STORAGE, ADAPTION OR ALTERATION, RETRIEVAL, CONSULTATION, USE, DISCLOSURE BY TRANSMISSION, DISSEMINATION, OR OTHERWISE MAKING AVAILABLE, ALIGNMENT OR COMBINATION, RESTRICTION, ERASURE, OR DESTRUCTION.

(H) "REASONABLE SECURITY PROCEDURES AND PRACTICES" MEANS SECURITY PROTECTIONS THAT ALIGN WITH THE CURRENT STANDARD OF CARE WITHIN SIMILAR COMMERCIAL ENVIRONMENTS AND WITH APPLICABLE STATE AND FEDERAL LAWS.

(I) "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.

(J) "SYSTEM" MEANS AN ELECTRONIC OR OTHER PHYSICAL MEDIUM MAINTAINED OR ADMINISTERED BY THE UNIVERSITY SYSTEM OF MARYLAND AND USED ON A PROCEDURAL BASIS TO STORE INFORMATION IN THE ORDINARY COURSE OF THE BUSINESS OF THE UNIVERSITY.

(K) "UNIVERSITY" MEANS THE UNIVERSITY SYSTEM OF MARYLAND.

10–13A–02.

(A) THIS SUBTITLE DOES NOT APPLY TO 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;

(4) IS DISCLOSED IN ACCORDANCE WITH THE FEDERAL FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT; OR

(5) IS CLINICAL INFORMATION RELATED TO SPONSORED RESEARCH.

(B) COMPLIANCE WITH THIS SUBTITLE DOES NOT AUTHORIZE THE UNIVERSITY SYSTEM OF MARYLAND TO FAIL TO COMPLY WITH ANY OTHER REQUIREMENTS OF STATE OR FEDERAL LAW RELATING TO THE PROTECTION AND PRIVACY OF PERSONALLY IDENTIFIABLE INFORMATION.

10–13A–03.

(A) THE UNIVERSITY SYSTEM OF MARYLAND SHALL REVIEW AND DESIGNATE SYSTEMS WITHIN THE UNIVERSITY AS SYSTEMS OF RECORD BASED ON THE FOLLOWING CRITERIA:

(1) THE RISK POSED TO INDIVIDUALS BY THE PERSONALLY

IDENTIFIABLE INFORMATION PROCESSED AND STORED ON THE SYSTEMS;

(2) THE RELATIONSHIP OF THE SYSTEMS TO THE OVERALL FUNCTION OF THE UNIVERSITY; AND

(3) THE TECHNICAL AND FINANCIAL FEASIBILITY OF IMPLEMENTING PRIVACY CONTROLS AND SERVICES WITHIN THE SYSTEM.

(B) THE UNIVERSITY SHALL DEVELOP AND ADOPT A PRIVACY GOVERNANCE PROGRAM TO GOVERN EACH SYSTEM OF RECORD THAT:

(1) IDENTIFIES AND DOCUMENTS THE PURPOSE OF THE UNIVERSITY IN PROCESSING PERSONALLY IDENTIFIABLE INFORMATION;

(2) PROHIBITS THE DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION TO THIRD PARTIES, OTHER THAN THOSE THIRD PARTIES PROCESSING PERSONALLY IDENTIFIABLE INFORMATION ON BEHALF OF THE UNIVERSITY, UNLESS:

(I) THE INDIVIDUAL CONSENTS TO DISCLOSURE OF THE INFORMATION; OR

(II) THE UNIVERSITY DETERMINES THAT DISCLOSURE OF THE INFORMATION IS IN THE BEST INTEREST OF THE UNIVERSITY;

(3) REQUIRES ALL AGREEMENTS ENTERED INTO WITH THIRD PARTIES ON OR AFTER OCTOBER 1, 2022, TO INCLUDE LANGUAGE REQUIRING THE THIRD PARTY TO SUPPORT THE UNIVERSITY'S PRIVACY GOVERNANCE PROGRAM;

(4) ENSURES THAT A THIRD PARTY PROCESSING PERSONALLY IDENTIFIABLE INFORMATION ON BEHALF OF THE UNIVERSITY ACTS IN ACCORDANCE WITH THE UNIVERSITY'S PRIVACY GOVERNANCE PROGRAM;

(5) TAKES REASONABLE STEPS TO ENSURE THAT PERSONALLY IDENTIFIABLE INFORMATION PROCESSED BY THE UNIVERSITY IS ACCURATE, RELEVANT, TIMELY, AND COMPLETE;

(6) TAKES REASONABLE STEPS TO ENSURE THAT REQUESTS TO ACCESS, MODIFY, OR DELETE INFORMATION AND REQUESTS TO OPT OUT OF THE SHARING OF INFORMATION WITH THIRD PARTIES ARE MADE BY THE SUBJECT OF THE PERSONALLY IDENTIFIABLE INFORMATION OR THE SUBJECT'S AGENT;

(7) TAKES REASONABLE STEPS TO LIMIT THE PERSONALLY

IDENTIFIABLE INFORMATION COLLECTED TO THAT INFORMATION NECESSARY TO ADDRESS THE PURPOSE OF THE COLLECTION;

(8) IMPLEMENTS A PROCESS TO PROVIDE INDIVIDUALS WITH ACCESS TO THE PERSONALLY IDENTIFIABLE INFORMATION RELATING TO THE INDIVIDUAL HELD AND PROCESSED BY THE UNIVERSITY;

(9) PROVIDES INDIVIDUALS WITH A PROCESS TO REQUEST A CORRECTION TO PERSONALLY IDENTIFIABLE INFORMATION RELATING TO THE INDIVIDUAL;

(10) IN THE CASE OF A DISAGREEMENT BETWEEN THE UNIVERSITY AND AN INDIVIDUAL OVER THE ACCURACY OF PERSONALLY IDENTIFIABLE INFORMATION RELATING TO THE INDIVIDUAL, PROVIDES A MEANS FOR THE INDIVIDUAL TO DOCUMENT THE DISAGREEMENT AND PRODUCE THE DOCUMENTATION OF THE DISAGREEMENT WHENEVER THE DISPUTED INFORMATION IS PRODUCED;

(11) PROVIDES A PROCESS FOR INDIVIDUALS TO REQUEST THE DELETION OF PERSONALLY IDENTIFIABLE INFORMATION RELATING TO THE INDIVIDUAL THAT THE UNIVERSITY DOES NOT HAVE A LEGITIMATE BASIS TO PROCESS;

(12) PROVIDES A PROCESS FOR INDIVIDUALS TO OPT OUT OF SHARING PERSONALLY IDENTIFIABLE INFORMATION RELATING TO THE INDIVIDUAL WITH THIRD PARTIES, IF THE UNIVERSITY WOULD NOT HAVE A LEGITIMATE BASIS TO PROCESS THE INFORMATION; AND

(13) PROVIDES A PROCESS FOR THE UNIVERSITY TO CONSIDER REQUESTS MADE UNDER THIS SUBSECTION THAT ALLOWS THE UNIVERSITY TO DENY A REQUEST IF THE UNIVERSITY REASONABLY CONCLUDES IT HAS A LEGITIMATE BASIS FOR PROCESSING THE PERSONALLY IDENTIFIABLE INFORMATION OR IF THE REQUEST IS NOT TECHNICALLY OR FINANCIALLY FEASIBLE.

(C) THE UNIVERSITY SHALL DEVELOP AND ADOPT AN INFORMATION SECURITY AND RISK MANAGEMENT PROGRAM FOR THE PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION THAT SHALL:

(1) IMPLEMENT REASONABLE SECURITY PROCEDURES AND PRACTICES, COMPATIBLE WITH APPLICABLE FEDERAL AND STATE STANDARDS AND GUIDELINES, TO ENSURE THAT THE RISK TO THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF ALL PERSONALLY IDENTIFIABLE INFORMATION IS PROPERLY MANAGED;

(2) BE PERIODICALLY ASSESSED BY A THIRD PARTY ASSESSOR WITH EXPERTISE IN INFORMATION SECURITY;

(3) BE APPROVED BY AN APPROPRIATE SENIOR OFFICIAL OF THE UNIVERSITY WITH AUTHORITY TO ACCEPT RISK FOR THE UNIVERSITY;

(4) REQUIRE THAT CONTRACTS WITH THIRD PARTIES INCLUDE PROVISIONS TO ENSURE THAT THIRD PARTIES THAT PROCESS PERSONALLY IDENTIFIABLE INFORMATION ON BEHALF OF THE UNIVERSITY MAINTAIN APPROPRIATE SECURITY CONTROLS COMMENSURATE WITH THE RISK POSED TO THE INDIVIDUALS BY THE PERSONALLY IDENTIFIABLE INFORMATION; AND

(5) ENSURE THAT ANY BREACHES BY THE UNIVERSITY OR A THIRD PARTY ACTING ON BEHALF OF THE UNIVERSITY ARE PROPERLY DOCUMENTED, INVESTIGATED, AND REPORTED TO APPROPRIATE AUTHORITIES WITHIN THE UNIVERSITY.

(D) (1) THE UNIVERSITY SHALL PUBLISH A PRIVACY NOTICE ON THE UNIVERSITY'S WEBSITE THAT IS:

(I) WRITTEN IN PLAIN LANGUAGE; AND

(II) DIRECTLY ACCESSIBLE FROM THE UNIVERSITY'S HOMEPAGE AND ANY OF THE UNIVERSITY'S WEBPAGES THAT ARE USED TO COLLECT PERSONALLY IDENTIFIABLE INFORMATION.

(2) THE NOTICE PUBLISHED UNDER PARAGRAPH (1) OF THIS SUBSECTION SHALL INCLUDE:

(I) THE TYPES OF PERSONALLY IDENTIFIABLE INFORMATION COLLECTED BY THE UNIVERSITY;

(II) THE PURPOSE OF THE COLLECTION, USE, AND SHARING OF PERSONALLY IDENTIFIABLE INFORMATION BY THE UNIVERSITY; AND

(III) THE PROCESSES BY WHICH AN INDIVIDUAL MAY REQUEST:

1. TO HAVE PERSONALLY IDENTIFIABLE INFORMATION RELATED TO THE INDIVIDUAL CORRECTED;

2. TO HAVE PERSONALLY IDENTIFIABLE INFORMATION RELATED TO THE INDIVIDUAL DELETED;

3. INFORMATION ON THE SHARING OF PERSONALLY IDENTIFIABLE INFORMATION BY THE UNIVERSITY WITH THIRD PARTIES, INCLUDING A LISTING OF THE THIRD PARTIES, A LISTING OF THE INFORMATION SHARED, AND THE PURPOSE OF SHARING THE INFORMATION; AND

4. TO OPT OUT OF THE SHARING OF PERSONALLY IDENTIFIABLE INFORMATION WITH A THIRD PARTY.

(3) THE UNIVERSITY SHALL ENSURE ACCESS CONTROLS ARE IN PLACE TO ADDRESS ANY SECURITY RISKS POSED BY PROVIDING THE NOTICE REQUIRED UNDER THIS SUBSECTION.

(E) WHEN THE UNIVERSITY IS DESTROYING RECORDS OF AN INDIVIDUAL THAT CONTAIN PERSONALLY IDENTIFIABLE INFORMATION OF THE INDIVIDUAL, THE UNIVERSITY SHALL TAKE REASONABLE STEPS TO PROTECT AGAINST UNAUTHORIZED ACCESS TO OR USE OF THE PERSONALLY IDENTIFIABLE INFORMATION, TAKING INTO ACCOUNT:

(1) THE SENSITIVITY OF THE RECORDS;

(2) THE NATURE OF THE UNIVERSITY AND ITS OPERATIONS;

(3) THE COSTS AND BENEFITS OF DIFFERENT DESTRUCTION METHODS; AND

(4) AVAILABLE TECHNOLOGY.

10–13A–04.

(A) IF THE UNIVERSITY COLLECTS PERSONALLY IDENTIFIABLE INFORMATION OF AN INDIVIDUAL AND DISCOVERS OR IS NOTIFIED OF A BREACH OF THE SECURITY OF A SYSTEM, THE UNIVERSITY SHALL CONDUCT IN GOOD FAITH A REASONABLE AND PROMPT INVESTIGATION TO DETERMINE WHETHER THE UNAUTHORIZED ACQUISITION OF PERSONALLY IDENTIFIABLE INFORMATION OF THE INDIVIDUAL HAS OCCURRED.

(B) (1) IF, AFTER THE INVESTIGATION IS CONCLUDED, THE UNIVERSITY DETERMINES THAT A BREACH OF THE SECURITY OF THE SYSTEM HAS OCCURRED, THE UNIVERSITY OR A THIRD PARTY, IF AUTHORIZED UNDER A WRITTEN CONTRACT OR AGREEMENT WITH THE UNIVERSITY, SHALL:

(I) NOTIFY THE INDIVIDUAL OF THE BREACH; AND

(II) NOTIFY THE UNIVERSITY'S CHIEF INFORMATION OFFICER OF THE BREACH.

(2) A NOTIFICATION REQUIRED UNDER PARAGRAPH (1) OF THIS SUBSECTION SHALL INCLUDE, TO THE EXTENT POSSIBLE, A DESCRIPTION OF THE CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION THAT WERE, OR ARE REASONABLY BELIEVED TO HAVE BEEN, ACQUIRED BY AN UNAUTHORIZED PERSON, INCLUDING WHICH OF THE ELEMENTS OF PERSONALLY IDENTIFIABLE INFORMATION WERE, OR ARE REASONABLY BELIEVED TO HAVE BEEN, ACQUIRED.

(3) IF THE UNIVERSITY DETERMINES THAT A BREACH OF THE SECURITY OF THE SYSTEM HAS OCCURRED INVOLVING THE PERSONALLY IDENTIFIABLE INFORMATION OF 1,000 OR MORE INDIVIDUALS, THE UNIVERSITY SHALL POST A NOTICE ON THE SAME WEBPAGE AS THE UNIVERSITY'S PRIVACY NOTICE WEBSITE:

(I) DESCRIBING THE BREACH; AND

(II) THAT REMAINS PUBLICLY AVAILABLE ON THE WEBSITE FOR AT LEAST 5 YEARS FROM THE DATE ON WHICH NOTICE WAS SENT TO INDIVIDUALS AFFECTED BY THE BREACH.

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2022.