PRINTER'S NO. 2617

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 2257 Session of 2022

INTRODUCED BY KENYATTA, SHUSTERMAN, GUENST, GALLOWAY, HILL-EVANS, BENHAM, SCHLOSSBERG, KINSEY, SAMUELSON, FREEMAN, SANCHEZ, HOWARD, ISAACSON, PARKER, MADDEN, O'MARA, NEILSON, GUZMAN, CIRESI, ZABEL, McNEILL, D. WILLIAMS, FITZGERALD, LEE AND DRISCOLL, JANUARY 20, 2022

REFERRED TO COMMITTEE ON CONSUMER AFFAIRS, JANUARY 20, 2022

AN ACT

Providing for protection of certain personal data of consumers; imposing duties on controllers and processors of personal data of consumers; providing for enforcement; prescribing penalties; and establishing the Consumer Privacy Fund.

TABLE OF CONTENTS

The General Assembly of the Commonwealth of Pennsylvania hereby enacts as follows:

CHAPTER 1

PRELIMINARY PROVISIONS

Section 101. Short title.

This act shall be known and may be cited as the Consumer Data Protection Act.

Section 102. Definitions.

The following words and phrases when used in this act shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"Affiliate," "affiliate of" or "person affiliated with." A person that directly or indirectly, through one or more intermediaries, controls, is controlled by or is under common control with a specified person. For the purposes of this definition, "control" or "controlled" means:

(1) ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting security of a company;

(2) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

(3) the power to exercise controlling influence over the management of a company.

"Authenticate." Verifying through reasonable means that a consumer, entitled to exercise the consumer rights under this act, is the same consumer exercising the consumer rights with respect to the personal data at issue.

"Automated means." A computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances, in whole or in part, without review or action by an individual.

"Biometric data." Data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. The term does not include a physical or digital photograph, a video or audio recording or data generated therefrom or information collected, used or stored for health care treatment, payment or operations under HIPAA.

"Breach of the security of the system" or "breach." The unauthorized access and acquisition of unencrypted data, or encrypted data with the confidential process or key required to decrypt the data, that is likely to compromise the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth. Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further authorized disclosure.

"Business associate."

(1) Except as provided in paragraph (4), business associate means, with respect to a covered entity, a person who:

(i) on behalf of such covered entity or of an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of the covered entity or arrangement, creates, receives, maintains or transmits protected health information for a function or activity regulated by this chapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities as defined in 42 CFR 3.20 (relating to definitions), billing, benefit management, practice management and repricing; or

(ii) provides, other than in the capacity of a member of the workforce of the covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) A person who is or does any of the following:

(i) A Health Information Organization, E-prescribing Gateway or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) Offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains or transmits protected health information on behalf of the business associate.

(4) The term does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent the activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) to

or for the organized health care arrangement by virtue of the activities or services.

"Child." An individual who is younger than 13 years of age.

"Consent." A clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to process personal data relating to the consumer. The act may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.

"Consumer." A natural person who is a resident of this Commonwealth acting only in a personal or household context. The term does not include a natural person who acts in a commercial or employment context.

"Controller." An entity that, alone or jointly with others, collects, uses, processes or stores personal information or directs others to collect, use, process or store personal information on its behalf.

"Covered entity." A covered entity means:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider that transmits health information in electronic form in connection with a transaction covered by this chapter.

"Data protection assessment." A process to identify and minimize the data protection risks of a project by:

(1) Describing the nature, scope, context and purpose of processing.

(2) Assessing necessity, proportionality and compliance measures.

(3) Identifying and assessing risk to individuals.

(4) Identifying additional measures to mitigate those

risks.

"Decision of the controller." A decision made by a controller to provide or deny a consumer's request for financial or lending services, housing, insurance, education enrollment, criminal justice, an employment opportunity, health care services or access to a basic necessity, such as food and water.

"De-identified data." Data that cannot reasonably be linked to an identified or identifiable individual or data on a device linked to the individual.

"Entity." An individual or business conducting business or other activities involving residents of this Commonwealth whether or not physically located in this Commonwealth or a Commonwealth agency or political subdivision of the Commonwealth.

"Financial institution." Any regulated financial institution insured by the Federal Deposit Insurance Corporation or its successor or an affiliate of the financial institution.

"Fund." The Consumer Privacy Fund established under section 503.

"Health care practitioner." An individual who is authorized to practice some component of the healing arts by a license, permit, certificate or registration issued by a Commonwealth licensing agency or board.

"Health care provider" or "provider." An individual, trust or estate, partnership, corporation (including associations, joint stock companies and insurance companies) or the Commonwealth or a political subdivision or instrumentality, including a municipal corporation or authority, thereof that operates a health care facility.

"Health record." A written, printed or electronically recorded material maintained by a health care entity in the course of providing health services to an individual concerning the individual and the services provided. The term includes the substance of a communication made by an individual to a health care entity in confidence during or in connection with the provision of health services or information otherwise acquired by the health care entity about an individual in confidence and in connection with the provision of health services to the individual.

"HIPAA." The Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191, 110 Stat. 1936).

"Identifiable private information." Any of the following:

(1) An individual's first name or first initial and last name in combination with and linked to one or more of the following data elements when the elements are not encrypted or redacted:

(i) Social Security number;

(ii) driver's license number;

(iii) State identification card number issued in lieu of a driver's license;

(iv) passport number;

(v) taxpayer identification number;

(vi) medical information;

(vii) health insurance information;

(viii) biometric data; or

(ix) a financial account number or a credit or debit card number in combination with other information that allows a financial, credit or debit account to be used or accessed.

(2) A data element enumerated in paragraph (1) if the information would reasonably permit the fraudulent assumption of the identity of an individual.

(3) An individual's username or e-mail address in combination with a password or security question and answer, biometric information or other information that would permit access to an online account.

(4) The term does not include information that an individual has made public himself or herself, information that the individual has consented in writing to be made public or information that was lawfully made public under Federal or State law or court order.

"Identified or identifiable natural person." An individual who can be readily identified, directly or indirectly.

"Institution of higher education." The term includes the following:

(1) A community college operating under Article XIX-A of the act of March 10, 1949 (P.L.30, No.14), known as the Public School Code of 1949.

(2) A university within the State System of Higher Education.

(3) The Pennsylvania State University.

(4) The University of Pittsburgh.

(5) Temple University.

(6) Lincoln University.

(7) Another institution that is designated as "State-related" by the Commonwealth.

(8) An accredited private or independent college or university.

(9) A private licensed school as defined in the act of

December 15, 1986 (P.L.1585, No.174), known as the Private Licensed Schools Act.

"International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use" or "(ICH)." An initiative that brings together regulatory authorities and the pharmaceutical industry to discuss scientific and technical aspects of pharmaceutical product development and registration.

"Minor." An individual who is under 18 years of age.

"Nonprofit organization." An organization exempt from taxation under section 501(c)(3), (6) or (12) of the Internal Revenue Code of 1986 (Public Law 99-514, 26 U.S.C. § 501(c)(3), (6) or (12)).

"Person." An individual.

"Personal data" or "consumer personal data." Information that is linked or reasonably linkable to an identified or identifiable natural person. The term does not include de-identified data or publicly available information.

"Precise geolocation data." Information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet. The term does not include the content of communications or data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a public utility.

"Process" or "processing." An operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion or modification of personal data.

"Processor." A person that processes personal data on behalf of a controller.

"Profiling." A form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

"Protected health information." As defined in 45 CFR 160.103 (relating to definitions).

"Pseudonymous data." Personal data that cannot be attributed to a specific natural person without the use of additional information, provided that the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

"Publicly available information." Information that:

(1) an individual has made public himself or herself;

(2) an individual has consented in writing to be made public;

(3) was lawfully made public under Federal or State law or court order; or

(4) is from another publicly available source, including news reports, periodicals, public social media posts or other widely distributed media.

"Qualified service organization." An entity that provides services such as data processing, bill collecting, dosage preparation, laboratory analysis or legal, accounting, population health management, medical staffing or other professional services or services to prevent or treat child abuse or neglect, including training on nutrition and child care

and individual and group therapy.

"Sale of personal data." The exchange of personal data for monetary consideration by a controller to a third party. The term does not include any of the following:

(1) The disclosure of personal data to a processor that processes the personal data on behalf of a controller.

(2) The disclosure of personal data to a third party for purposes of providing a product or service requested by a consumer.

(3) The disclosure or transfer of personal data to an affiliate of a controller.

(4) The disclosure of information that a consumer:

(i) intentionally made available to the general public through publicly available sources, including news reports, periodicals, public social media posts or other widely distributed media; and

(ii) did not restrict disclosure to a specific audience.

(5) The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction in which the third party assumes control of all or part of the controller's assets.

"Sensitive data." A category of personal data that includes any of the following:

(1) personal data revealing racial or ethnic origin, religious beliefs, mental behavioral or physical health diagnosis, sexual orientation, gender or gender identity, citizenship or immigration status;

(2) the processing of genetic or biometric data for the

purpose of uniquely identifying a natural person;

(3) the personal data collected from a minor; or

(4) precise geolocation data.

"Targeted advertising." Displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from the consumer's online activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests. The term does not include any of the following:

(1) Advertisements based on activities within a controller's own websites or online applications.

(2) Advertisements based on the context of a consumer's current search query, visit to a website or online application.

(3) Advertisements directed to a consumer in response to the consumer's request for information or feedback.

(4) Processing personal data processed solely for measuring or reporting advertising performance, reach or frequency.

"Third party." A person, other than a consumer, controller or processor or an affiliate of a processor or controller. The term shall include an agency of the Federal Government, a Commonwealth agency or a local agency.

"Third party controller or processor." A person or entity acting on behalf of a controller or processor.

Section 103. Applicability.

(a) General rule.--This act applies to persons that conduct business in this Commonwealth or produce goods, products or services that are sold or offered for sale to residents of this Commonwealth and that:

(1) during a calendar year, control or process personal data of at least 100,000 consumers; or

(2) control or process personal data of at least 25,000 consumers and derive over 50% of gross revenue from the sale of personal data.

(b) Nonapplicability.--This act shall not apply to any of the following:

(1) The Commonwealth or a political subdivision of the Commonwealth or an agency, office, authority, board, bureau or commission of the Commonwealth or a political subdivision.

(2) A financial institution or data subject to Title V of the Gramm-Leach-Bliley Act (Public Law 106-102, 113 Stat. 1338).

(3) A covered entity or business associate of a covered entity governed by the privacy, security and breach notification rules issued by the Department of Health and Human Services under 45 CFR Pts. 160 (relating to general administrative requirements) and 164 (relating to security and privacy) established under HIPAA, and Title XIII of the American Recovery and Reinvestment Act of 2009 (Public Law 111-5, 123 Stat. 115).

(4) A nonprofit organization.

(5) An institution of higher education.

(c) Exempt information and data.--The following information and data is exempt from this act:

(1) Protected health information under HIPAA.

(2) Health records as defined by and for lawful purposes under State law.

(3) Patient identifying information for purposes of section 522 of the Public Health Service Act (58 Stat. 682,

42 U.S.C. § 290dd-2).

(4) Identifiable private information for purposes of the Federal policy for the protection of human subjects under 45 CFR Pt. 46 (relating to protection of human subjects), identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by The International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use or the protection of human subjects under 21 CFR Pts. 50 (relating to protection of human subjects) and 56 (relating to institutional review boards) or personal data used or shared in research conducted in accordance with the requirements specified in this act or other research conducted in accordance with applicable law.

(5) Information and documents created for purposes of the Health Care Quality Improvement Act of 1986 (Public Law 99-660, 42 U.S.C. § 11101 et seq.).

(6) Patient safety work product for purposes of the Patient Safety and Quality Improvement Act of 2005 (Public Law 109-41, 42 U.S.C. § 299 et seq.).

(7) Information derived from any of the health care-related information that is de-identified in accordance with the requirements for de-identification under HIPAA.

(8) Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as information exempt under this subsection that is maintained by a covered entity or business associate of a covered entity as defined by HIPAA or a program or a qualified service organization as defined by section 522 of

the Public Health Services Act.

(9) Information used only for public health activities and purposes as authorized by HIPAA.

(10) The collection, maintenance, disclosure, sale, communication or use of personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, business or public utility that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that the activity is regulated by and authorized under the Fair Credit Reporting Act (Public Law 91-508, 15 U.S.C. § 1681 et seq.).

(11) Data collected, processed, sold or disclosed in compliance with 18 U.S.C. § 2721 (relating to prohibition on release and use of certain personal information from State motor vehicle records).

(12) Personal data regulated by the Family Educational Rights and Privacy Act of 1974 (Public Law 90-247, 20 U.S.C. § 1232g).

(13) Personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act of 1971 (Public Law 92-181, 12 U.S.C. § 2001 et seq.).

(14) Data processed or maintained:

(i) to the extent that data is collected and used in the course of employment with, or the performance of, a contract for a controller, processor or third party;

(ii) as the emergency contact information of an individual under this act used for emergency contact purposes; or

(iii) as necessary to retain or administer benefits for another individual relating to the individual under subparagraph (i) and used for the purposes of administering those benefits.

(d) Compliance under other Federal law.--A controller or processor that complies with the verifiable parental consent requirements of the Children's Online Privacy Protection Act (Public Law 105-277, 15 U.S.C. § 6501 et seq.) shall be deemed compliant with any obligation to obtain parental consent under this act.

CHAPTER 3

ENUMERATION OF RIGHTS AND RESPONSIBILITIES

Section 301. Rights of consumers and controllers.

(a) Consumer rights.--A consumer may invoke the consumer rights authorized under this subsection at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to invoke. A known child's parent or legal guardian may invoke the consumer rights on behalf of the child regarding processing personal data belonging to the known child. The consumer may invoke the right:

(1) To confirm whether or not the controller is processing the consumer's personal data and to access the personal data.

(2) To correct inaccuracies in the consumer's personal data.

(3) To delete personal data provided by the consumer or obtained by the controller about the consumer.

(4) To obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily

usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means.

(5) To opt out of the processing of the personal data for purposes of:

(i) targeted advertising;

(ii) the sale of personal data; or

(iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

(b) Controller duties.--Except as otherwise provided in this act, a controller shall comply with a request by a consumer to exercise the consumer rights authorized under subsection (a) as follows:

(1) The controller shall respond to the consumer within 45 days of receipt of a request submitted under subsection (a). The response period may be extended once by 45 additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of the extension within the initial 45-day response period, together with the reason for the extension.

(2) If the controller declines to take action regarding a consumer's request, the controller shall:

(i) inform the consumer within 45 days of receipt of the request of the justification for declining to take action; and

(ii) provide the consumer with instructions on how to appeal the decision under subsection (c).

(3) (i) Information provided in response to a

consumer's request to invoke consumer rights shall, except as provided in subparagraph (ii), be provided by the controller free of charge and up to twice annually per consumer.

(ii) If a request from a consumer is determined by the comptroller to be unfounded, excessive or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller shall bear the burden of demonstrating that a consumer's request under subsection (a) is unfounded, excessive or repetitive.

(4) If the controller is unable to authenticate the request using reasonable efforts, the controller may not be required to comply with a request to initiate an action under subsection (a). The controller may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

(c) Appeal process.--

(1) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision.

(2) The appeal process shall be stated in plain language. The controller shall respond to the consumer within 45 days of receipt of the appeal, notifying the consumer that the appeal has been received.

(3) Within 60 days of receipt of an appeal, the controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a

written explanation of the reasons for the decisions.

(4) If the appeal is denied, the controller shall provide the consumer with an online form that the consumer may use to contact the Attorney General to submit a complaint. Information about the form shall be published on a publicly accessible Internet website.

Section 302. Controller responsibilities.

(a) General rule.--A controller shall:

(1) Limit the collection of personal data to what is necessary in relation to the purposes for which the data is collected, processed and maintained by the controller, as disclosed to the consumer.

(2) Except as otherwise provided in this act, not collect and process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which the personal data is collected, processed and maintained, as disclosed to the consumer, unless the controller obtains the consumer's prior consent.

(3) Establish, implement and maintain reasonable administrative, technical data security practices to protect the confidentiality, integrity and accessibility of personal data. The data security practices shall be appropriate to the volume and nature of all consumer personal data collected, processed and maintained by the controller.

(4) (i) Not process personal data in violation of Federal and State laws that prohibit unlawful discrimination against consumers, including the act of December 17, 1968 (P.L.1224, No.387), known as the Unfair Trade Practices and Consumer Protection Law. A controller shall not discriminate against a consumer by:

(A) exercising a consumer right under section 301(a);

(B) denying goods, products or services;

(C) charging different prices or rates for goods, products or services; or

(D) providing a different level of quality of goods and services to the consumer.

(ii) Nothing in this paragraph shall be construed to require a controller to:

(A) provide a good, product or service that requires the personal data of a consumer that the controller does not collect or maintain in the normal course of business or otherwise; or

(B) prohibit a controller from offering a different price, rate, level, quality or selection of goods, products or services to a consumer, including offering goods, products or services for no fee, if the consumer has exercised the right to opt out under this act or the offer is related to a consumer's voluntary participation in a bona fide loyalty, promotional, rewards, premium features, discounts or club card program or any other similar program.

(5) Not process sensitive data concerning a consumer without obtaining the consumer's written consent or, in the case of the processing of sensitive data concerning a known child, without processing the data in accordance with the Children's Online Privacy Protection Act (Public Law 105-277, 15 U.S.C. § 6501 et seq.).

(b) Void contract provisions.--A provision of a contract or agreement that purports to waive or limit a consumer right under

this act shall be deemed contrary to the intent and policy purposes of this act and shall be void and unenforceable.

(c) Consumer notice from controller.--

(1) A controller shall provide a consumer with an accessible, clear and meaningful privacy notice that includes:

(i) The categories of personal data collected, processed and maintained by the controller.

(ii) The purpose for processing the consumer's personal data.

(iii) How the consumer may exercise the consumer's rights under section 301, including how the consumer may appeal the controller's decision with regard to a consumer's request under section 301(a).

(iv) The categories of personal data that the controller shares with third parties, if any.

(v) The categories of third parties, if any, with whom the controller shares personal data.

(2) The privacy notice shall be provided to the consumer by United States Postal Service mail, annually, and shall be accessible, electronically on the controller's publicly accessible Internet website.

(d) Disclosure of sale and advertising processes.--If a controller sells consumer personal data to third parties or processes consumer personal data for targeted advertising, the controller shall clearly and conspicuously disclose the sale or processing, to the affected consumers, as well as the manner in which a consumer may opt out of the sale and processing of the consumer's personal data under this subsection.

(e) Privacy notice.--

(1) A controller shall establish and describe in a privacy notice the reliable procedures a consumer may use to submit a request to exercise the consumer rights under this act. The procedures shall take into account:

(i) the ways in which a consumer normally communicates or interacts with the controller;

(ii) the need for secure and reliable communication of the request; and

(iii) the method the controller will use to authenticate the identity of the consumer making a request.

(2) The controller shall not require a consumer with an existing account to create a new account in order to exercise a consumer right under this act.

Section 303. Responsibility of processors.

(a) Processors.--A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this act. The assistance shall include:

(1) Technical and organizational measures that take into account the nature of processing consumer personal data and the information available to the processor, as reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests under section 301.

(2) Security measures that take into account the nature of processing consumer personal data and the information available to the processor, in order to assist the controller in meeting the controller's obligations in relation to the security of processing consumer personal data and in relation to the notification of a breach of the security of the system

of the processor.

(3) Providing necessary information to enable the controller to conduct and document data protection assessments.

(b) Contract between controllers and processors.--

(1) A contract between a controller and a processor shall include provisions to govern the processor's data processing procedures with respect to the processing of consumer personal data performed by a processor on behalf of a controller.

(2) A contract under this subsection shall:

(i) be binding;

(ii) clearly state instructions for processing data, including the nature and purpose of processing, and the type of data subject to processing;

(iii) indicate the duration of processing; and

(iv) specify the rights and obligations of both the controller and the processor.

(3) The contract shall also include requirements that the processor shall:

(i) Ensure that a person processing consumer personal data is informed of and subject to confidentiality requirements under Federal laws and regulations and the laws and regulations of this Commonwealth with respect to the data.

(ii) At the controller's direction, delete and return all consumer personal data to the controller as requested at the end of the contract, unless retention of the personal data is required by law.

(iii) Upon the request of the controller, make

available to the controller all information in the processor's possession necessary to demonstrate the processor's compliance with the processor's obligations under this act.

(iv) Allow, and cooperate with, audits by the controller or the controller's designated assessor or, alternatively, allow the processor to arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this act using an appropriate and accepted control standard or framework and assessment procedure for the assessment. The processor shall provide a report of the assessment to the controller upon request.

(4) In order to meet a processor's obligations to a controller, a processor may contract with a subcontractor to process consumer personal data in accordance with the requirements of this act. A contract entered into under this paragraph shall include provisions informing the subcontractor of the confidentiality requirements under Federal laws and regulations and State laws and regulations and making the subcontractor subject to the confidentiality requirements.

(5) A subcontractor under paragraph (4) shall be subject to all the requirements that relate to the obligations of a processor under this act.

(c) Construction.--Nothing in this section shall be construed to relieve a controller or a processor and a contractor or subcontractor under subsection (b) from the liabilities imposed on such controller, processor, contractor or

subcontractor by virtue of their roles in the processing of consumer personal data under this act.

Section 304. Data protection assessments.

(a) Duty of controller.--A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

(1) The processing of personal data for purposes of targeted advertising.

(2) The sale of personal data.

(3) The processing of personal data for purposes of profiling, where the profiling presents a reasonably foreseeable risk of:

(i) discriminatory, unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

(ii) financial, physical or reputational injury to consumers;

(iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where the intrusion would be offensive to a reasonable person; or

(iv) other substantial injury to consumers.

(4) The processing of sensitive data.

(5) Any processing activity involving personal data that presents a heightened risk of harm to consumers.

(b) Identification and weighing of benefits.--

(1) Data protection assessments conducted under subsection (a) shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other persons and the public against the potential risks to the rights of the consumer

associated with the processing, as mitigated by safeguards that can be employed by the controller to reduce the risks.

(2) The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into the assessment by the controller.

(c) Authority of Attorney General.--

(1) The Attorney General may request by subpoena that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General.

(2) The Attorney General may evaluate the data protection assessment for compliance with the responsibilities specified in this act.

(3) Data protection assessments shall be confidential and exempt from public inspection and copying.

(4) The disclosure of a data protection assessment as a result of a request from the Attorney General shall not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

(d) Comparable set of processing operations permitted.--A single data protection assessment may address a comparable set of processing operations that include similar activities.

(e) Compliance with other laws.--A data protection assessment conducted by a controller for the purpose of compliance with Federal or State laws or regulations may comply under this section if the assessment has a reasonably comparable

scope and effect.

(f) Applicability.--Data protection assessment requirements shall apply to processing activities created or generated after January 1, 2023, and are not retroactive.

Section 305. Processing de-identified data and exemptions.

(a) Duties of controller.--The controller in possession of de-identified data shall:

(1) Take reasonable measures to ensure that the data cannot be associated with a natural person.

(2) Publicly commit to maintaining and using de-identified data without attempting to re-identify the data.

(3) Contractually obligate a recipient of the de-identified data to comply with all provisions of this act.

(b) Construction.--Nothing in this act shall be construed to require a controller or processor to:

(1) Re-identify de-identified data or pseudonymous data; or maintain data in identifiable form, or collect, obtain, retain or access any data or technology in order to be capable of associating an authenticated consumer request with personal data.

(2) Require a controller or processor to comply with an authenticated consumer rights request under this act if all of the following are true:

(i) The controller is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data.

(ii) The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the

personal data with other personal data about the same consumer.

(iii) The controller does not sell the personal data to a third party or otherwise voluntarily disclose the personal data to a third party other than a processor, except as otherwise permitted in this act.

(c) Pseudonymous data.--The consumer rights contained in this act shall not apply to pseudonymous data in a case where the controller is able to demonstrate that information necessary to identify the consumer is maintained separately from the original data and is secured in such a way that prevents the controller from accessing the information.

(d) Duty to exercise reasonable oversight.--A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with safety standards, contracts with consumer, and Federal and State laws to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address a breach of the contractual commitment.

Section 306. Limitations.

(a) General rule.--Nothing in this act shall be construed to restrict a controller's or processor's ability to:

(1) Comply with Federal, State or local law, rule or regulation.

(2) Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by a Federal, State, local or other governmental authority.

(3) Cooperate with a law enforcement agency concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate Federal,

State or local law, rule or regulation.

(4) Investigate, establish, exercise, prepare for or defend a legal claim.

(5) Provide a good, product or service specifically requested by a consumer, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer prior to entering into a contract.

(6) Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual, and where the processing cannot be manifestly based on another legal basis.

(7) Prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity, preserve the integrity or security of data systems or investigate, report or prosecute a person responsible for that action.

(8) Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other Federal, State or local ethics and privacy laws and is approved, monitored and governed by an independent oversight entity that determines:

(i) if the deletion of the information is likely to provide substantial benefits to the consumer that do not exclusively accrue to the controller;

(ii) the expected benefits of the research outweigh the privacy risks; and

(iii) the controller has implemented reasonable safeguards to mitigate privacy risks associated with

research, including risks associated with re-identification.

(9) Assist another controller, processor or third party with an obligation under this subsection.

(b) Other abilities preserved.--The obligations imposed on controllers or processors under this act shall not be construed to restrict a controller's or processor's ability to collect, use or retain data to:

(1) Conduct internal research to develop, improve or repair products, services or technology.

(2) Effectuate a product recall.

(3) Identify and repair technical errors that impair existing or intended functionality of the data.

(4) Perform internal operations that are reasonably aligned with the expectations of a consumer or reasonably anticipated by a consumer based on a consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a good, product or service specifically requested by a consumer or the performance of a contract to which a consumer is a party.

(c) Evidentiary privileges.--

(1) The obligations imposed on controllers or processors under this act shall not apply where compliance by the controller or processor with this act would violate an evidentiary privilege under the laws of this Commonwealth.

(2) Nothing in this act shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of this Commonwealth as part of a

privileged communication.

(d) Defenses.--

(1) A controller or processor that discloses personal data to a third-party controller or processor in compliance with the requirements of this act is not in violation of this act if the third-party controller or processor that receives and processes the personal data is in violation of this act, provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation.

(2) A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this act is not in violation of this act for the transgressions of the controller or processor from which it receives the personal data.

(e) Construction.--Nothing in this act shall be construed as imposing an obligation on a controller or processor that adversely affects the right or freedom of a person, such as exercising the right of free speech pursuant to the First Amendment to the Constitution of the United States, or applies to the processing of personal data by a person in the course of a purely personal or household activity.

(f) Permissible processing.--

(1) Personal data processed by a controller or processor under contract with a controller under this section shall not be processed for any purpose other than those expressly listed in this section unless otherwise allowed by this act. Personal data processed by a controller or processor under contract with a controller under this section may be processed to the extent that such processing is:

(i) Reasonably necessary and proportionate to the purposes listed in this section.

(ii) Limited to what is necessary in relation to the specific purposes listed in this section.

(2) Personal data collected, used or retained under subsection (b) shall, where applicable, take into account the nature and purpose or purposes of the collection, use or retention. The data shall be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use or retention of personal data.

(g) Controller burden to demonstrate exemption.--If a controller processes personal data by virtue of an exemption under this section, the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with the requirements of subsection (f).

(h) Status as controller.--Processing personal data for the purposes expressly identified in subsection (a) shall not solely make an entity a controller with respect to the processing.

CHAPTER 5

ADMINISTRATION AND ENFORCEMENT

Section 501. Powers and duties of Attorney General.

(a) Administration.--The Attorney General shall administer and enforce the provisions of this act and may adopt regulations to carry out the requirements of this act.

(b) Investigative authority.--Whenever the Attorney General has reasonable cause to believe that a person has engaged in, is engaging in or is about to engage in a violation of this act,

the Attorney General may issue a civil investigative demand.

Section 502. Enforcement procedure.

(a) Notice of violation.--Prior to initiating an action under this act, the Attorney General shall provide a controller or processor 30 days' written notice identifying the specific provisions of this act that the Attorney General alleges have been or are being violated.

(b) Cure of violation.--If within the 30-day period specified under subsection (b), the controller or processor cures the noticed violation and provides the Attorney General an express written statement that the alleged violations have been cured and that no further violations shall occur, no action shall be initiated against the controller or processor.

(c) Failure to cure.--If a controller or processor continues to violate this act following the cure period in subsection (b) or breaches an express written statement provided to the Attorney General under this section, the Attorney General may initiate an action in the name of the Commonwealth and may seek an injunction to restrain the violation of this act and civil penalties of up to $7,500 for each violation under this act.

(d) Recovery of reasonable expenses.--The Attorney General may recover reasonable expenses incurred in investigating and preparing the case, including attorney fees, in an action initiated under this act.

(e) Construction.--Nothing in this act shall be construed as providing the basis for, or be subject to, a private right of action for violations of this act or under any other law.

Section 503. Consumer Privacy Fund.

(a) Establishment.--The Consumer Privacy Fund is established in the State Treasury.

(b) Contents of fund.--All civil penalties, expenses and attorney fees collected under this act shall be paid into the State Treasury and credited to the fund. Interest earned on money in the fund shall remain in the fund and shall be credited to the fund. Any money remaining in the fund, including interest, at the end of each fiscal year shall not revert to the General Fund but shall remain in the fund.

(c) Use of fund.--The money in the fund shall be used by the Office of the Attorney General to enforce the provisions of this act.

CHAPTER 7

MISCELLANEOUS PROVISIONS

Section 701. (Reserved).

Section 702. Effective date.

This act shall take effect January 1, 2023, or in 18 months, whichever is later.