PRIOR PRINTER'S NOS. 1272, 2315 PRINTER'S NO. 2442

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 1201 Session of 2023

INTRODUCED BY NEILSON, SCIALABBA, C. WILLIAMS, GAYDOS, CIRESI, McNEILL, KHAN, SANCHEZ, KINSEY, CEPEDA-FREYTIZ, PARKER, HILL-EVANS, GALLOWAY, GREEN, WAXMAN, OTTEN AND N. NELSON, MAY 19, 2023

AS AMENDED ON SECOND CONSIDERATION, HOUSE OF REPRESENTATIVES, DECEMBER 13, 2023

AN ACT

Providing for consumer data privacy, for duties of controllers and for duties of processors; and imposing penalties.

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

Section 1. Short title.

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

Section 2. 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." A legal entity that shares common branding with another legal entity or controls, is controlled by or is under common control with another legal entity.

"Biometric data." Data generated by automatic measurements of an individual's biological characteristics, including fingerprints, voiceprints, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. The term does not include a digital or physical photograph, an audio or video recording or any data generated from a digital or physical photograph or an audio or video recording. The term does not include information captured and converted to a mathematical representation, including a numeric string or similar method that cannot be used to recreate the data captured or converted to create the mathematical representation.

"Business associate." As defined in 45 CFR 160.103 (relating to definitions)

"Child." As defined in 15 U.S.C. § 6501 (relating to definitions).

"Common branding." A shared name, servicemark or trademark.

"Consent." A clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer. The term includes a written statement, including by electronic means, or any other unambiguous affirmative action specified in this definition. The term does not include acceptance of general or broad terms of use or a similar document that contains descriptions of personal data processing along with other unrelated information, hovering over, muting, pausing or closing a given piece of content or an agreement obtained through the use of dark patterns.

"Consumer." An individual who is a resident of this Commonwealth. The term does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with a controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency.

"Control." Any of the following:

(1) Ownership of or the power to vote on more than 50% of the outstanding shares of any class of voting security of a controller.

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

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

"Controller." As follows:

(1) A sole proprietorship, partnership, limited liability company, corporation, association or other legal entity that meets all of the following criteria:

(i) Is organized or operated for the profit or financial benefit of its shareholders or other owners.

(ii) Alone or jointly with others, determines the purposes and means of the processing of consumers' personal information.

(iii) Does business in this Commonwealth.

(iv) Satisfies any of the following thresholds:

(A) Has annual gross revenues in excess of $10,000,000.

(B) Alone or in combination, annually buys or receives, sells or shares for commercial purposes, alone or in combination, the personal information of at least 50,000 consumers, households or devices.

(C) Derives at least 50% of annual revenues from selling consumers' personal information.

(2) An entity that controls a sole proprietorship, partnership, limited liability company, corporation, association or other legal entity under paragraph (1) ~~and~~ OR **<--** shares common branding with the sole proprietorship, partnership, limited liability company, corporation, association or other legal entity.

"Covered entity." As defined in 45 CFR 160.103.

"Dark pattern." A user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making or choice, including a practice the Federal Trade Commission refers to as a dark pattern.

"Decisions that produce legal or similarly significant effects concerning the consumer." Decisions made by a controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services.

"De-identified data." Data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual or a device linked to the individual, if the controller that possesses the data complies with the following criteria:

(1) Takes reasonable measures to ensure that the data cannot be associated with an individual.

(2) Publicly commits to process the data only in a de-identified fashion and not attempt to re-identify the data.

(3) Contractually obligates a recipient of the data to satisfy the criteria specified under paragraphs (1) and (2).

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

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

"Institution of higher education." As defined in section 118(c) of the act of March 10, 1949 (P.L.30, No.14), known as the Public School Code of 1949.

"Nonprofit organization." An organization that is exempt from taxation under 26 U.S.C. § 501(c)(3), (4), (6) or (12) (relating to exemption from tax on corporations, certain trusts, etc.).

"Personal data." As follows:

(1) Any information that is linked or reasonably linkable to an identified or identifiable individual.

(2) The term does not include publicly available information, de-identified data or biometric data captured and converted to a mathematical representation.

"Precise geolocation data." Information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, that directly identify 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 any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

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

"Processing activities that present a heightened risk of harm to a consumer." The term includes any of the following:

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

(2) The sale of personal data.

(3) The processing of personal data for the purpose of profiling if the profiling presents a reasonably foreseeable risk of any of the following:

(i) Unfair or deceptive treatment of, or an unlawful disparate impact on, a consumer.

(ii) Financial, physical or reputational injury to a consumer.

(iii) A physical or other intrusion upon the solitude or seclusion of a consumer or the private affairs or concerns of a consumer where the intrusion would be offensive to a reasonable person.

(iv) Any other substantial injury to a consumer.

(4) The processing of sensitive data.

"Processor." An individual who, or legal entity that, processes personal data on behalf of a controller.

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

"Protected health information." As defined in 45 CFR 160.103.

"Pseudonymous data." Personal data that cannot be attributed to a specific individual without the use of additional information if 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 individual.

"Publicly available information."

Information that:

(1) is lawfully available through Federal, State or municipal records or widely distributed media; or

(2) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public.

"Sale of personal data." The exchange of personal data for monetary or other valuable 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 the controller.

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

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

(4) The disclosure of personal data when a consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party.

(5) The disclosure of personal data that a consumer:

(i) intentionally made available to the general public via a channel of mass media; and

(ii) did not restrict to a specific audience.

(6) 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 or a proposed merger, acquisition, bankruptcy or other transaction, in which the third party assumes control of all or part of the controller's assets.

"Sensitive data." Personal data that includes data revealing any of the following:

(1) A racial or ethnic origin.

(2) Religious beliefs.

(3) Mental or physical health condition or diagnosis.

(4) Sex life or sexual orientation.

(5) Citizenship or immigration status.

(6) The processing of genetic or biometric data for the purpose of uniquely identifying an individual.

(7) Personal data collected from a known child.

(8) Precise geolocation data.

"Targeted advertising." Displaying advertisements to a consumer if the advertisement is selected based on personal data obtained or inferred from the consumer's activities over time and across nonaffiliated Internet 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 Internet websites or online applications.

(2) Advertisements based on the context of a consumer's current search query, visit to an Internet 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 solely to measure or report

advertising frequency, performance or reach.

"Third party." An individual or legal entity, including a public authority, agency or body, other than a consumer, controller or processor or an affiliate of the processor or the controller.

"Trade secret." As defined in 12 Pa.C.S. § 5302 (relating to definitions).

Section 3. Consumer data privacy.

(a) Rights of consumers.--A consumer shall have the right to do the following:

(1) Confirm whether or not a controller is processing or accessing the consumer's personal data, unless the confirmation or access would require the controller to reveal a trade secret.

(2) Correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.

(3) Delete personal data provided by or obtained about the consumer.

(4) Obtain a copy of the consumer's personal data processed by a 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 in a manner that would disclose the controller's trade secrets.

(5) Opt out of the processing of the consumer's personal data for the purpose of any of the following:

(i) Targeted advertising.

(ii) The sale of personal data, except as provided under section 5(b).

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

(b) Exercise of rights.--A consumer may exercise the rights under subsection (a) by a secure and reliable means established by a controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent in accordance with section 4 to exercise the consumer's right under subsection (a)(5) to opt out of the processing of the consumer's personal data on behalf of the consumer. For processing personal data of a known child, the parent or legal guardian may exercise the consumer's rights under subsection (a) on the child's behalf. For processing personal data concerning a consumer subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the consumer may exercise the consumer's rights under subsection (a) on the consumer's behalf.

(c) Compliance.--Except as otherwise provided in this act, a controller shall comply with a request by a consumer to exercise the consumer's rights under subsection (a) as follows:

(1) The controller shall respond to the consumer without undue delay, but no later than 45 days after receipt of the request. The controller may extend the response period under this paragraph by an additional 45 days when reasonably necessary, considering the complexity and number of the consumer's requests, if the controller informs the consumer of the extension within the initial 45-day response period and the reason for the extension.

(2) If the controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but no later than 45 days after receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision.

(3) Information provided in response to consumer requests shall be provided by the controller, free of charge, once per consumer during a 12-month period. If a request from a consumer is manifestly 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 bears the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

(4) If a controller is unable to authenticate a request to exercise a right afforded under subsection (a)(1), (2), (3) or (4) using commercially reasonable efforts, the controller shall not be required to comply with a request under this subsection and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise the right until the consumer provides additional information reasonably necessary to authenticate the consumer and the consumer's request to exercise the right. A controller shall not be required to authenticate an opt-out request under subsection (a)(5), but the controller may deny an opt-out request if the controller has a good faith, reasonable and documented belief that the request is fraudulent. If a controller denies an opt-out request under subsection (a)(5) because the controller believes the request is fraudulent, the controller shall send a notice to the

person who made the request disclosing that the controller believes the request is fraudulent, why the controller believes the request is fraudulent and that the controller will not comply with the request.

(5) A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete the personal data in accordance with subsection (a)(3) by retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring that the consumer's personal data remains deleted from the controller's records and not using such retained data for any other purpose in accordance with the provisions of this act or opting the consumer out of the processing of the data for any purpose except for those exempted under section 11(a)(3).

(d) Appeals.--A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request by a consumer to exercise the consumer's rights under subsection (a) within a reasonable period of time after the consumer's receipt of the decision under subsection (c)(2). The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate an action under subsection (b). No later than 60 days after receipt of an appeal, the controller shall inform the consumer in writing of an action taken or not taken in response to the appeal, including a written explanation of the reason for the decision. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

Section 4. Designation of authorized agent.

A consumer may designate another person to serve as the consumer's authorized agent and act on the consumer's behalf to opt out of the processing of the consumer's personal data for the purposes specified under section 3(a)(5). A controller shall comply with an opt-out request received from an authorized agent under section 3(a)(5) if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

Section 5. Duties of controllers.

(a) Duties.--A controller shall have all of the following duties:

(1) Limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer.

(2) Except as otherwise provided in this act, refrain from processing personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.

(3) Process personal data in a manner that ensures reasonable and appropriate administrative, technical, organizational and physical safeguards of personal data collected, stored and processed.

(4) Refrain from processing sensitive data concerning a consumer without obtaining the consumer's consent or, in the case of the processing of sensitive data concerning a known

child, without processing the data, in accordance with 15 U.S.C. Ch. 91 (relating to children's online privacy protection).

(5) Refrain from processing personal data in violation of a Federal or State law that prohibits unlawful discrimination against a consumer.

(6) Provide an effective mechanism for a consumer to revoke the consumer's consent that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of the consent, cease to process the data as soon as practicable, but no later than 15 days after the receipt of the request.

(7) Refrain from processing the personal data of a consumer for the purpose of targeted advertising or selling the consumer's personal data without the consumer's consent under circumstances where the controller has actual knowledge and willfully disregards that the consumer is younger than 16 years of age.

(8) Refrain from discriminating against a consumer for exercising any of the consumer rights under section 3(a), including denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods or services to the consumer.

(b) Construction.--Nothing in subsection (a) shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain nor prohibit a controller from offering a different price, rate, level, quality or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts or club card program.

(c) Privacy notice.--A controller shall provide a consumer with a reasonably accessible, clear and meaningful privacy notice that includes all of the following:

(1) The categories of personal data processed by the controller.

(2) The purpose for processing personal data.

(3) How the consumer may exercise the consumer's rights, including how the consumer may appeal the controller's decision with regard to the consumer's request under section 3(d).

(4) The categories of personal data that the controller shares with each third party.

(5) The categories of each third party with which the controller shares personal data.

(6) An active email address or other online mechanism that the consumer may use to contact the controller.

(d) Disclosures.--If a controller sells personal data to a third party or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the sale or processing and the manner in which a consumer may exercise the right to opt out of the sale or processing.

(e) Means to exercise rights.--

(1) A controller shall establish and describe in the privacy notice under subsection (c) a secure and reliable means for consumers to submit a request to exercise the consumer's rights under section 3(a). The secure and reliable

means under this paragraph shall take into account the manner in which a consumer normally interacts with the controller, the need for secure and reliable communication for the request and the ability of the controller to verify the identity of the consumer making the request. A controller may not require a consumer to create a new account in order to exercise the consumer's rights under section 3(a), but may require the consumer to use an existing account. The secure and reliable means shall include all of the following:

(i) Providing a clear and conspicuous link on the controller's Internet website to an Internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising or sale of the consumer's personal data under section 3(a)(5).

(ii) No later than January 1, 2026, allowing a consumer to opt out of the processing of the consumer's personal data for the purpose of targeted advertising or the sale of the consumer's personal data under section 3(a)(5) through an opt-out preference signal sent, with the consumer's consent, by a platform, technology or mechanism to the controller indicating the consumer's intent to opt out of the processing or sale. The platform, technology or mechanism shall comply with all of the following criteria:

(A) Not unfairly disadvantage another controller.

(B) Not make use of a default setting, but instead require the consumer to make an affirmative, freely given and unambiguous choice to opt out of the processing or sale of the consumer's personal data.

(C) Be consumer friendly and easy to use by the average consumer.

(D) Be as consistent as possible with any other similar platform, technology or mechanism required by a Federal or State law or regulation.

(E) Enable the controller to accurately determine whether the consumer is a resident of this Commonwealth and whether the consumer has made a legitimate request to opt out of processing or sale of the consumer's personal data.

(F) Be in compliance with this section. A controller that recognizes signals approved by other states shall be considered in compliance with this section.

(iii) If a consumer's decision to opt out of the processing of the consumer's personal data for the purpose of targeted advertising or the sale of the consumer's personal data under section 3(a)(5) through an opt-out preference signal sent under subparagraph (ii) conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's bona fide loyalty, rewards, premium features, discounts or club card program, the controller shall comply with the consumer's opt-out preference signal, but may notify the consumer of the conflict and provide to the consumer the choice to confirm the controller-specific privacy setting or participation in the program.

(2) If a controller responds to a consumer's opt-out request under paragraph (1)(i) by informing the consumer of a

charge for the use of a product or service, the controller shall present the terms of a bona fide loyalty, rewards, premium features, discounts or club card program for the retention, use, sale or sharing of the consumer's personal data.

Section 6. Duties of processors.

(a) Assistance.--A processor shall adhere to the instructions of a controller and shall assist the controller in complying with the controller's duties under this act. The assistance shall include all of the following:

(1) Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as is reasonably practicable, to fulfill the controller's duty to comply with a request by a consumer to exercise the consumer's rights under section 3(a).

(2) Taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's duties in relation to the security of processing the personal data and in relation to the notification of a breach of security of the system of the processor.

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

(b) Contracts.--A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly state the instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. The contract shall also require that the processor comply with all of the following:

(1) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data.

(2) At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by Federal or State law.

(3) Upon the reasonable 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 provisions of this act.

(4) After providing the controller with an opportunity to object, engage a subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

(5) Allow and cooperate with a reasonable assessment by the controller or the controller's designated assessor, or 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 requirements 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.

(c) Construction.--Nothing in this section shall be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of the role of the controller or processor in the processing relationship specified under this act.

(d) Acting as controller or processor.--A determination of whether a person is acting as a controller or processor with respect to a specific processing of data shall be a fact-based determination that depends upon the context in which personal data is to be processed. The following shall apply:

(1) A person who is not limited in the person's processing of personal data pursuant to a controller's instructions or who fails to adhere to the instructions shall be a controller and not a processor with respect to a specific processing of data.

(2) A processor who continues to adhere to a controller's instructions with respect to a specific processing of personal data shall remain a processor.

(3) If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor shall be a controller with respect to the processing and may be subject to an enforcement action under section 10.

Section 7. Data protection assessment.

(a) Assessment.--A controller shall conduct and document a data protection assessment for each of the controller's processing activities that present a heightened risk of harm to a consumer.

(b) Benefits and risks.--In conducting a data protection assessment under subsection (a), a controller shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the consumer's rights under section 3(a) associated with the processing, as mitigated by safeguards that can be employed by the controller to reduce the risks. The controller shall factor all of the following into the data protection assessment:

(1) The use of de-identified data.

(2) The reasonable expectations of the consumer.

(3) The context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(c) Availability of assessments.--The Attorney General may require a controller to disclose a data protection assessment under subsection (a) 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. The Attorney General may evaluate a data protection assessment for compliance with the provisions of this act. A data protection assessment shall be confidential and exempt from disclosure under 5 U.S.C. § 552 (relating to public information; agency rules, opinions, orders, records, and proceedings) and the act of February 14, 2008 (P.L.6, No.3), known as the Right-to-Know Law. To the extent that information contained in a data protection assessment disclosed to the Attorney General under this subsection includes information subject to attorney-client privilege or work product protection, the disclosure shall not constitute a waiver of the privilege or protection.

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

(e) Compliance.--If a controller conducts a data protection assessment for the purpose of complying with another applicable Federal or State law or regulation, the data protection assessment shall be deemed to satisfy the requirements under this section if the data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted under this section.

(f) Applicability.--The data protection assessment requirements under this section shall apply to processing activities created or generated after July 1, 2024, and shall not apply retroactively.

Section 8. De-identified and pseudonymous data.

(a) Duties.--A controller in possession of de-identified data shall have the following duties:

(1) Take reasonable measures to ensure that the de-identified data cannot be associated with an individual.

(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 the provisions of this act.

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

(1) require a controller or processor to re-identify de-identified data or pseudonymous data;

(2) maintain data in identifiable form or collect, obtain, retain or access data or technology in order to be capable of associating an authenticated consumer rights request under section 3(a); or

(3) comply with an authenticated consumer rights request

under section 3(a) if the controller:

(i) 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 consumer's personal data;

(ii) does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data or does not associate the personal data with other personal data about the same specific consumer; and

(iii) 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 authorized under this section.

(c) Pseudonymous data.--The consumer rights specified under section 3(a)(1), (2), (3) or (4) shall not apply to pseudonymous data if a controller is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

(d) Oversight.--A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with a contractual commitment 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 9. Exemptions on restrictions for controllers or processors.

(a) Legal compliance.--Nothing in this act shall be construed to restrict the ability of a controller or processor to:

(1) comply with Federal or State laws or local ordinances or regulations;

(2) comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by a Federal, State, municipal or other governmental authority;

(3) cooperate with a law enforcement agency concerning a conduct or activity that the controller or processor reasonably and in good faith believes may violate a Federal or State law or local ordinance or regulation;

(4) investigate, establish, exercise, prepare for or defend legal claims;

(5) provide a product or service specifically requested by a consumer;

(6) perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;

(7) take steps at the request of a consumer prior to entering into a contract;

(8) take immediate steps to protect an interest that is essential for the life or physical safety of a consumer or another individual, including when processing cannot be manifestly based on the provisions of this act;

(9) prevent, detect, protect against or respond to a security incident, identity theft, fraud, harassment, malicious or deceptive activity or illegal activity, preserve the integrity or security of a system or investigate, report or prosecute an individual responsible for an incident specified under this paragraph;

(10) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to

all other applicable Federal or State ethics and privacy laws and is approved, monitored and governed by an institutional review board or a similar independent oversight entity that determines whether:

(i) the deletion of information is likely to provide substantial benefits to the research 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 the research, including risks associated with re-identification;

(11) assist another controller, processor or third party with any of the requirements under this act; or

(12) process personal data for reasons of public interest in the area of public health, community health or population health, but solely to the extent that the processing is:

(i) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed; and

(ii) under the responsibility of a professional subject to confidentiality obligations under Federal or State law or local ordinance.

(b) Data collection.--The requirements imposed on a controller or processor under this act shall not restrict the ability of a controller or processor to collect, use or retain data for internal use for any of the following purposes:

(1) Conducting internal research to develop, improve or

repair products, services or technology.

(2) Effectuating a product recall.

(3) Identifying and repairing technical errors that impair existing or intended functionality.

(4) Internal operations that are reasonably aligned with the expectations of a consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer.

(c) Evidentiary privilege.--The requirements imposed on a controller or processor under this act shall not apply if compliance by the controller or processor with requirements would violate an evidentiary privilege under the laws of this Commonwealth. Nothing in this act shall be construed to prevent a controller or processor from providing personal data concerning a consumer to an individual covered by an evidentiary privilege under the laws of this Commonwealth as part of a privileged communication.

(d) Third parties.--A controller or processor that discloses personal data to a third-party controller or third-party processor in accordance with this act shall not be deemed to have violated the provisions of this act if the third-party controller or third-party processor violates the provisions of this act if, at the time of the disclosure, the disclosing controller or processor did not have actual knowledge that the third-party controller or third-party processor would violate the provisions of this act. A third-party controller or third-party processor who receives personal data under this subsection in accordance with this act shall not be deemed to have violated the provisions of this act for a violation by the disclosing controller or processor.

(e) Individual liberties.--Nothing in this act shall be construed to:

(1) impose an obligation on a controller or processor that adversely affects the rights or freedoms of an individual, including the freedom of speech or freedom of the press guaranteed in the First Amendment to the Constitution of the United States or section 7 of Article I of the Constitution of Pennsylvania; or

(2) apply to an individual's processing of personal data in the course of the individual's purely personal or household activities.

(f) Personal data.--

(1) Personal data processed by a controller may be processed to the extent that the processing meets all of the following criteria:

(i) Is reasonably necessary and proportionate to the purposes specified under this section.

(ii) Is adequate, relevant and limited to what is necessary in relation to the specific purposes specified under this section.

(2) A controller or processor that collects, uses or retains personal data under subsection (b) shall, when applicable, take into account the nature and purpose of the collection, use or retention of the personal data. The personal data under subsection (b) shall be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and reduce reasonably foreseeable risks of

harm to a consumer related to the collection, use or retention of the personal data.

(g) Exemptions.--If a controller processes personal data in accordance with an exemption under this section, the controller shall be responsible for demonstrating that the processing qualifies for the exemption and complies with the requirements under subsection (f).

(h) Legal entities.--The processing of personal data for the purposes expressly specified under this section shall not solely make a legal entity a controller with respect to the processing.

Section 10. Penalties, enforcement and private rights of action.

(a) Enforcement.--The Attorney General shall have exclusive authority to enforce the provisions of this act. The following shall apply:

(1) During the period beginning July 1, 2024, and ending December 31, 2025, the Attorney General shall, prior to initiating an action for a violation of a provision of this act, issue a notice of violation to the controller or processor if the Attorney General determines that a cure is possible. If the controller fails to cure the violation within 60 days of receipt of the notice of violation, the Attorney General may initiate an action under this section.

(2) Beginning January 1, 2026, the Attorney General may, in determining whether to grant a controller or processor the opportunity to cure an alleged violation under paragraph (1), consider all of the following:

(i) The number of violations.

(ii) The size and complexity of the controller or processor.

(iii) The nature and extent of the processing activities of the controller or processor.

(iv) The substantial likelihood of injury to the public.

(v) The safety of persons or property.

(vi) Whether the alleged violation was likely caused by human or technical error.

(3) The right to cure shall apply for 60 days.

(b) Private rights of action.--Nothing in this act shall be construed as providing the basis for a private right of action for a violation of the provisions of this act.

(c) Unfair trade practice.--Violations of the provisions of this act shall constitute "unfair methods of competition" and "unfair or deceptive acts or practices" under the act of December 17, 1968 (P.L.1224, No.387), known as the Unfair Trade Practices and Consumer Protection Law, and shall be enforced exclusively by the Attorney General.

(d) Regulations.--The Attorney General shall promulgate regulations necessary to implement this section.

Section 11. Nonapplicability, exemption and consent.

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

(1) The Commonwealth or any of its political subdivisions.

(2) A nonprofit organization.

(3) An institution of higher education.

(4) A national securities association that is registered under 15 U.S.C. § 78o-3 (relating to registered securities associations).

(5) A financial institution or an affiliate of a

financial institution or data subject to Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.).

(6) A covered entity or business associate.

(b) Exemptions.--The following shall be exempt from the provisions of this act:

(1) Protected health information under HIPAA.

(2) Patient-identifying information for purposes of 42 U.S.C. § 290dd-2 (relating to confidentiality of records).

(3) Identifiable private information for purposes of the Federal policy for the protection of human subjects under 45 CFR Subt. A Subch. A Pt. 46 (relating to protection of human subjects).

(4) Identifiable private information that is otherwise information collected as part of human subjects research in accordance with the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use on the effective date of this paragraph.

(5) The protection of human subjects under 21 CFR Ch. I Subch. A Pt. 50 (relating to protection of human subjects) or 56 (relating to institutional review boards) or personal data used or shared in research, as defined in 45 CFR 164.501 (relating to definitions), that is conducted in accordance with the standards specified under this subsection or other research conducted in accordance with applicable Federal or State law.

(6) Information and documents created for the purposes of 42 U.S.C. Ch. 117 (relating to encouraging good faith professional review activities).

(7) Patient safety work product for the purposes of 42

U.S.C. Ch. 6A Subch. VII Pt. C (relating to patient safety improvement).

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

(9) 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, program or qualified service organization as specified in 42 U.S.C. § 290dd-2 (relating to confidentiality of records).

(10) Information used for public health activities and purposes as authorized by HIPAA, community health activities and population health activities.

(11) 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, furnisher or user that provides information for use in a consumer report or by a user of a consumer report, but only to the extent that the activity is regulated by and authorized under 15 U.S.C. Ch. 41 Subch. III (relating to credit reporting agencies).

(12) Personal data collected, processed, sold or disclosed in compliance with 18 U.S.C. Ch. 123 (relating to prohibition on release and use of certain personal information from state motor vehicle records).

(13) Personal data regulated by 20 U.S.C. Ch. 31 Subch.

III Pt. 4 (relating to records; privacy; limitation on withholding Federal funds).

(14) Personal data collected, processed, sold or disclosed in compliance with 12 U.S.C. Ch. 23 (relating to farm credit system).

(15) Data processed or maintained:

(i) in the course of an individual applying to, employed by or acting as an agent or independent contractor of a controller, processor or third party to the extent that the data is collected and used within the context of that role;

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

(iii) as necessary to administer benefits for another individual related to an individual who is the subject of the information under paragraph (1) and used for the purposes of administering the benefits.

(16) Personal data collected, processed, sold or disclosed in relation to price, route or service by an air carrier under 49 U.S.C. Subt. VII Pt. A. Subpt. I Ch. 401 (relating to general provisions) to the extent preempted under 49 U.S.C. § 41713 (relating to preemption of authority over prices, routes, and service).

(c) Parental consent.--A controller or processor that complies with the verifiable parental consent requirements under 15 U.S.C. Ch. 91 (relating to children's online privacy protection) shall be deemed compliant with an obligation to obtain parental consent under this act.

Section 12. Effective date.

This act shall take effect in six months.