PRINTER'S NO. 2481

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 1947 Session of 2024

INTRODUCED BY MERCURI, SCIALABBA, PICKETT, JAMES, CIRESI, KEEFER, KUTZ, GLEIM, ZIMMERMAN AND JOZWIAK, JANUARY 9, 2024

REFERRED TO COMMITTEE ON CONSUMER PROTECTION, TECHNOLOGY AND UTILITIES, JANUARY 9, 2024

AN ACT

Providing for consumer data privacy, for rights of consumers and duties of businesses relating to the collection of personal information and for duties of the Attorney General.

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:

"Biometric information." Personal information generated from the measurement or specific technological processing of an individual's unique biological, physical or physiological characteristics, including any fingerprint, voice print, iris or retina scan, facial scan or template, deoxyribonucleic acid (DNA) information or gait. The term does not include any writing

sample, written signature, photograph, voice recording, video, demographic data or physical characteristics, including height, weight, hair color or eye color, if the information is not used for the purpose of identifying an individual's unique biological, physical or physiological characteristics.

"Business." The following:

(1) A sole proprietorship, partnership, limited liability company, corporation, association or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected, that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in this Commonwealth and that satisfies one or more of the following thresholds:

(i) Has annual gross revenues in excess of $25,000,000.

(ii) Alone or in combination, annually buys, receives for the business's commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 100,000 or more consumers.

(iii) Derives 50% or more of annual revenues from selling consumers' personal information.

(2) An entity that controls, is controlled by or is under common control with a business under paragraph (1) or shares common branding with the business.

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

"Consent." A clear and affirmative act, including a written or electronic statement, signifying a consumer's freely given,

specific, informed and unambiguous agreement to the processing of personal information. The term does not include any of the following:

(1) Acceptance of general or broad terms of use or a similar document that contains descriptions of personal information processing with other unrelated information.

(2) Hovering over, muting, pausing or closing a piece of content.

(3) An agreement obtained through use of a design, modification or manipulation of a user interface with the purpose or substantial effect of obscuring, subverting or impairing user autonomy, decision making or choice as specified in the regulations promulgated under section 3(n).

"Consumer." An individual who is a resident of this Commonwealth acting only in the context of the individual or the individual's household. The term does not include an individual acting in a commercial or employment context, as a job applicant or as a beneficiary of an individual acting in an employment context.

"Control." Ownership of or the power to vote on more than 50% of the outstanding shares of any class of voting security of a business, control in any manner over the election of a majority of the directors, or of individuals exercising similar functions, or the power to exercise a controlling influence over the management of a company.

"Decisions that produce legal or similarly significant effects." Decisions that result in the provision or denial of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services or access to basic necessities, including food or

water.

"Deidentified." 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 and is possessed by a business that:

(1) takes reasonable measures to ensure that the data cannot be associated with the individual;

(2) publicly commits to maintain and use the data only in a deidentified manner and not attempt to reidentify the data; and

(3) contractually obligates a recipient of the data to meet the criteria specified in this definition.

"Personal information." Information that identifies or could reasonably be linked, directly or indirectly, with a particular consumer, household or consumer device. The term does not include any of the following:

(1) Information that is lawfully made available from Federal, State or local government records.

(2) Consumer information that is deidentified or aggregate consumer information.

"Process" or "processing." Any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means, including the collection, use, storage, disclosure, analysis, deletion or modification of personal information.

"Profiling." A form of automated processing of personal information to evaluate, analyze or predict personal aspects concerning an identified individual or identifiable individual, including the individual's economic situation, health, personal preferences, interests, reliability, behavior, location or

movements.

"Publicly available." Information that is lawfully made available from Federal, State or local government records or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience. The term does not include biometric information collected by a business about a consumer without the consumer's knowledge or consumer information that is deidentified or aggregate consumer information.

"Sale," "sell" or "sold." The exchange of personal information for monetary or other valuable consideration by a business to a third party. The term does not include any of the following:

(1) The disclosure of personal information to a service provider that processes the personal information on behalf of a business.

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

(3) The disclosure or transfer of personal information to an affiliate of a business.

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

(5) The disclosure of personal information that:

(i) a consumer directs a business to disclose or intentionally discloses by using the business to interact with a third party; or

(ii) is intentionally made available by a consumer to the general public via a channel of mass media unless the consumer has restricted the information to a specific audience.

"Service provider." A person that processes personal information on behalf of a business.

"Targeted advertising." Displaying to a consumer an advertisement that is selected based on personal information obtained or inferred during a period of time from the consumer's activities across nonaffiliated Internet websites, applications or online services to predict consumer preferences or interests. The term does not include any of the following:

(1) Advertising to a consumer in response to the consumer's request for information or feedback.

(2) Advertising based on activities within a business's own Internet website or online applications.

(3) Advertising based on the context of a consumer's current search query or visit to an Internet website or online application.

"Third party." Any person, public authority, public agency, entity or body other than a consumer, business, service provider or an affiliate of the business or service provider.

Section 3. Consumer data privacy.

(a) General rule.--A consumer shall have the right to:

(1) Know whether a business is processing personal information about the consumer.

(2) Know whether the consumer's personal information is

processed for the purpose of targeted advertising or the sale of personal information.

(3) Decline or opt out of the processing of the consumer's personal information for the purpose of any of the following:

(i) Targeted advertising.

(ii) The sale of personal information.

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

(4) Access the consumer's personal information.

(5) Correct inaccurate personal information concerning the consumer, taking into account the nature of the personal information and the purpose of the processing of the personal information.

(6) Request that a business delete personal information that the business processes about the consumer. The following shall apply to this paragraph:

(i) A business that collects personal information about a consumer shall disclose under subsection (l) the consumer's right to request the deletion of the consumer's personal information.

(ii) Except as otherwise provided under this act, a business that receives a verifiable request from a consumer to delete the consumer's personal information shall delete the consumer's personal information from its records and direct a service provider who processes the consumer's personal information on the business's behalf to delete the personal information within 45 calendar days.

(7) Obtain personal information previously provided by the consumer to the business in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the personal information to another business without hindrance, when the processing of the personal information is carried out by automated means.

(b) Disclosure by businesses.--A business shall provide a consumer with a reasonably accessible, clear and meaningful privacy notice, including the following:

(1) The categories of personal information the business processes.

(2) The categories of sources from which the personal information is collected.

(3) The purpose for processing the categories of personal information.

(4) The categories of personal information that the business shares with a third party, if applicable.

(5) The specific pieces of personal information the business has collected about the consumer.

(6) How and where the consumer may exercise the consumers' rights provided under this act.

(7) If the business sells personal information to a third party or processes personal information for targeted advertising, the sale or processing and the manner in which a consumer may exercise the consumer's right to opt out of the sale or processing.

(c) Request from consumer.--Nothing in this section shall be construed to require a business to:

(1) retain any personal information about a consumer collected for a single one-time transaction if, in the

ordinary course of business, that information about the consumer is not retained; or

(2) reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

(d) Consumers of young age.--A business may not process a consumer's personal information for the purpose of targeted advertising or the sale of personal information if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of a consumer who is between 13 and 16 years of age, or the consumer's parent or guardian, in the case of a consumer who is less than 13 years of age, has consented to the processing. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age.

(e) Duties of care.--A business or service provider shall implement and maintain reasonable security procedures and practices, including administrative, physical and technical safeguards, appropriate to the nature of the personal information and the purposes for which the personal information will be used, to protect consumers' personal information from unauthorized use, disclosure, access, destruction or modification.

(f) Duties of data minimization.--A business's collection of personal information shall be adequate, relevant and limited to what is reasonably necessary regarding the purpose for which the personal information is processed.

(g) Duties to avoid secondary use.--Except as provided under this act, a business may not process personal information for a purpose that is not reasonably necessary to, or compatible with,

the purpose for which the personal information is processed unless the business obtains the consumer's consent.

(h) Duties to avoid unlawful discrimination.--A business may not process personal information in violation of a Federal or State law that prohibits unlawful discrimination against consumers.

(i) Discrimination prohibited.--

(1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this section, including, but not limited to, by:

(i) Denying goods or services to the consumer.

(ii) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(iii) Providing a different level or quality of goods or services to the consumer.

(iv) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(2) Nothing in this subsection shall prohibit a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data.

(j) Exercise of rights.--A business shall:

(1) In a form that is reasonably accessible to consumers, make available to consumers two or more designated methods for submitting verifiable requests to exercise the rights specified under subsection (a), including, but not limited to, a publicly accessible Internet website.

(2) Respond to a consumer's verifiable request under paragraph (1) free of charge within 45 days of receiving the verifiable request from the consumer. The time period to respond to the verifiable request may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. A business shall not be required to provide the information required under subsection (l) to a consumer more than once during a 12-month period.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices are informed of the requirements of this section and how to direct consumers to exercise their rights.

(4) For a consumer who exercises the consumer's right to opt out of the processing of the consumer's personal information for the purpose of targeted advertising or the sale of personal information, refrain from processing the personal information for the purpose of targeted advertising or the sale of personal information unless the consumer subsequently consents to the processing. This paragraph shall apply to a consumer who communicates or signals the consumer's right to opt out via user-enabled global privacy controls, including browser plug-in or privacy settings, device settings or any other mechanism.

(5) For a consumer who exercises the consumer's right to opt out of the processing of the consumer's personal information for the purpose of targeted advertising or the sale of personal information, respect the consumer's decision to opt out for a period of no less than 12 months before requesting the consumer's consent to the processing.

(6) Use personal information collected from the consumer in relation to the consumer's verifiable request under paragraph (1) for the sole purpose of complying with the verifiable request.

(k) Obligations on business.--

(1) The obligations imposed on a business or service provider under this section shall not restrict the ability of a business or service provider to:

(i) Comply with Federal, State or local laws.

(ii) Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by Federal, State or local authorities.

(iii) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider or third party reasonably and in good faith believes may violate Federal, State or local laws.

(iv) Exercise or defend legal claims.

(v) Collect, use, retain, sell or disclose consumer information that is deidentified.

(vi) Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of this Commonwealth. For purposes of this section, commercial conduct takes place wholly outside of this Commonwealth if the business collected that information while the consumer was outside of this Commonwealth, no part of the sale of the consumer's personal information occurred in this Commonwealth and no personal information collected while the consumer was in this Commonwealth is sold. This subparagraph shall not permit a business to store,

including on a device, personal information about a consumer when the consumer is in this Commonwealth and then collecting that personal information when the consumer and stored personal information is outside of this Commonwealth.

(vii) Provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party or take steps at the request of the consumer before entering into the contract or offer a voluntary bona fide loyalty or rewards program.

(viii) Take immediate steps to protect an interest that is essential for the life of the consumer or another individual if the processing cannot otherwise be authorized under this act.

(ix) Prevent, detect, protect against or respond to a security incident, identity theft, fraud, harassment, a malicious or deceptive activity or an illegal activity to preserve the integrity or security of the system or to investigate, report or prosecute a person responsible for an activity specified under this subparagraph.

(x) Engage in public or peer-reviewed scientific, historical or statistical research in the public interest that adheres to applicable Federal and State laws and is approved, monitored and governed by an institutional review board, human subjects research ethics review board or a similar independent oversight entity, which determines all of the following:

(A) If the research is likely to provide substantial benefits that do not exclusively accrue to the controller.

(B) If the expected benefits of the research outweigh the privacy risks.

(C) If the controller has implemented reasonable safeguards to mitigate privacy risks associated with the research, including any risks associated with reidentification.

(2) The obligations imposed on a business or service provider under this section shall not restrict the ability of a business or service provider to collect, use or retain information for any of the following purposes:

(i) Conducting internal research to improve, repair or develop products, services or technology.

(ii) Performing internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the business.

(3) The obligations imposed on a business or service provider under this section shall not do any of the following:

(i) Apply when compliance by the business or service provider would violate an evidentiary privilege provided under the laws of this Commonwealth.

(ii) Prevent a business or service provider from providing personal information concerning a consumer to an individual covered by an evidentiary privilege provided under the laws of this Commonwealth as part of a privileged communication.

(iii) Adversely affect the rights of an individual provided under the Constitution of the United States or the Constitution of Pennsylvania.

(iv) Apply to the processing of personal information by an individual in the course of only a personal or household activity.

(v) Apply to specific data that is under the purview of the Gramm-Leach-Bliley Act (Public Law 106-102, 113 Stat. 1338) or the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191, 110 Stat. 1936).

(4) If a business or service provider processes personal information in accordance with this subsection, the business or service provider shall have the burden of demonstrating that the processing meets the requirements under this subsection.

(5) Personal information that is processed by a business or service provider under this act may not be processed for any purpose other than a purpose authorized under this subsection.

(6) Personal information that is processed by a business or service provider under this act may be processed only to the extent that the processing:

(i) is necessary, reasonable and proportionate for a purpose authorized under this subsection;

(ii) is adequate, relevant and limited to a purpose authorized under this subsection; and

(iii) to the extent possible, adheres to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal information and to reduce reasonably foreseeable risks of harm to the consumer.

(l) Duties of businesses and service providers.--

(1) A business or service provider shall meet the obligations imposed under this act.

(2) A service provider shall adhere to the instructions of a business and assist the business to meet the business's obligations under this act. Based on the nature of the processing and the information available to the service provider, the service provider shall assist the business by engaging in all of the following:

(i) To the extent possible, taking appropriate technical and organizational measures to satisfy the business's obligation to respond to a consumer request to exercise the consumer's rights under subsection (a).

(ii) Assisting the business in meeting the business's obligations regarding the security of processing personal information and notice of a breach of the security of the system in accordance with the act of December 22, 2005 (P.L.474, No.94), known as the Breach of Personal Information Notification Act.

(3) Notwithstanding the instructions of a business, a service provider shall have the following duties:

(i) Ensuring that each person processing personal information is subject to a duty of confidentiality with respect to the information.

(ii) Engaging a subcontractor, after providing the business with an opportunity to object in accordance with a written contract under paragraph (5), that requires the subcontractor to meet the obligations of the service provider regarding the personal information.

(4) Based on the context of the processing, a business and a service provider shall implement appropriate technical

and organizational measures to ensure a level of security appropriate to the risk and clearly allocate the duties to implement the measures.

(5) The processing by a service provider shall be governed by a binding written contract between the business and the service provider that provides for all of the following provisions:

(i) The processing instructions for the service, including the nature and purpose of the processing.

(ii) The type of personal information subject to the processing and the duration of the processing.

(iii) The requirements imposed under this paragraph and paragraphs (3) and (4).

(iv) At the request of the business, the service provider shall delete or return the personal information to the business at the end of the provision of services, unless retention of the personal information is required by the laws of this Commonwealth.

(v) The service provider shall make available to the business all information necessary to demonstrate compliance with the obligations under this act.

(vi) Except as provided under subparagraph (vii), the service provider shall allow for and contribute to reasonable audits and inspections by the business or the business's designated auditor.

(vii) In lieu of complying with subparagraph (vi), the service provider may, with the business's consent, arrange for a qualified and independent auditor to conduct, at least annually and at the service provider's expense, an audit of the service provider's policies and

technical and organizational measures in support of the obligations under this act. An auditor shall use an appropriate and accepted control standard or framework and audit procedure for an audit under this subparagraph. Upon request by the business, the service provider shall provide a report of an audit under this subparagraph to the business.

(viii) The contract may not relieve the business or service provider from the liabilities imposed on the business or service provider regarding processing under this act.

(ix) The determination whether a person is acting as the business or service provider regarding processing is a fact-based determination that depends on the context in which personal information is processed. A person who is not limited in the processing of personal information, in accordance with the business's instructions, or who fails to adhere to the business's instructions, shall be considered a business regarding the processing of the personal information. A service provider that continues to adhere to the business's instructions regarding the processing of personal information shall remain the service provider. If a service provider determines, by itself or in collaboration with another person, the purpose and means of the processing of personal information, the service provider shall be considered a business regarding the processing.

(6) A business or service provider that discloses personal information to another business or service provider in compliance with this act shall not be in violation of this

act if all of the following apply:

(i) The recipient processes the personal information in violation of this act.

(ii) At the time of disclosing the personal information, the business or service provider did not have actual knowledge that the recipient intended to commit a violation of this act.

(7) A business or service provider that receives personal information from another business or service provider in compliance with this act as specified under paragraph (6) shall not be in violation of this act if another business or service provider fails to comply with applicable obligations under this act.

(m) Violation.--A business shall be in violation of this section if the business fails to cure an alleged violation within 60 days after being notified of alleged noncompliance. A business that fails to cure an alleged violation within 60 days after being notified of alleged noncompliance shall be in violation of the act of December 17, 1968 (P.L.1224, No.387), known as the Unfair Trade Practices and Consumer Protection Law. A business, service provider or any other person that violates this section shall be subject to an injunction and liable for a civil penalty of not more than $2,500 for each unintentional violation and not more than $7,500 for each intentional violation. Nothing in this act shall be construed to create or imply a private cause of action.

(n) Rules and regulations.--The Attorney General shall promulgate rules and regulations to implement this section and may provide publicly available opinions for the purpose of promoting the effective compliance with this act.

Section 4. Effective date.

This act shall take effect in one year.