STATE OF NEW YORK

5642

2019-2020 Regular Sessions

IN SENATE

May 9, 2019

Introduced by Sens. THOMAS, CARLUCCI, MYRIE -- read twice and ordered printed, and when printed to be committed to the Committee on Consumer Protection

AN ACT to amend the general business law, in relation to the management and oversight of personal data

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. Short title. This act may be known and cited as the "New York privacy act".

§ 2. The general business law is amended by adding a new article 42 to read as follows:

ARTICLE 42

NEW YORK PRIVACY ACT

Section 1100. Definitions.

1101. Jurisdictional scope.

1102. Data fiduciary.

1103. Consumer rights.

1104. Transparency.

1105. Responsibility according to role.

1106. De-identified data.

1107. Exemptions.

1108. Liability.

1109. Enforcement.

1110. Preemption.

§ 1100. Definitions. The definitions in this article apply unless the context clearly requires otherwise:

1. "Affiliate" means a legal entity that controls, is controlled by, or is under common control with, another legal entity, where the entity holds itself out as affiliated or under common ownership such that a consumer acting reasonably under the circumstances would anticipate their personal data being provided to an affiliate.

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD10868-05-9

2. "Consent" means a clear affirmative act establishing a freely given, specific, informed, and unambiguous indication of a consumer's agreement to the processing of personal data relating to the consumer, such as by a written statement or other clear affirmative action.

3. "Consumer" means a natural person who is a New York resident. It does not include an employee or contractor of a business acting in their role as an employee or contractor.

4. "Controller" means the natural or legal person who, alone or jointly with others, determines the purposes and means of the processing of personal data.

5. "Data broker" means a business, or unit or units of a business, separately or together, that earns its primary revenue from supplying data or inferences about people gathered mainly from sources other than the data sources themselves.

6. "De-identified data" means:

(a) data that cannot be linked to a known natural person without additional information not available to the controller; or

(b) data (i) that has been modified to a degree that the risk of re-identification is small as determined by a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for de-identifying data, (ii) that is subject to a public commitment by the controller not to attempt to re-identify the data, and (iii) to which one or more enforceable controls to prevent re-identification has been applied. Enforceable controls to prevent re-identification may include legal, administrative, technical, or contractual controls.

7. "Developer" means a person who creates or modifies the set of instructions or programs instructing a computer or device to perform tasks.

8. "Identified or identifiable natural person" means a person who can be identified, directly or indirectly, in particular by reference to specific information including, but not limited to, a name, an identification number, specific geolocation data, or an online identifier.

9. "Minor" means any person under eighteen years of age.

10. "Personal data" means information relating to an identified or identifiable natural person.

(a) "Personal data" includes:

(i) an identifier such as a real name, alias, signature, date of birth, gender identity, sexual orientation, marital status, physical characteristic or description, postal address, telephone number, unique personal identifier, military identification number, online identifier, Internet Protocol address, email address, account name, mother's maiden name, social security number, driver's license number, passport number, or other similar identifier;

(ii) information such as employment, employment history, bank account number, credit card number, debit card number, insurance policy number, or any other financial information, medical information, mental health information, or health insurance information;

(iii) commercial information, including a record of personal property, income, assets, leases, rentals, products or services purchased, obtained, or considered, or other purchasing or consuming history;

(iv) biometric information, including a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry;

(v) internet or other electronic network activity information, including browsing history, search history, content, including text, photographs, audio or video recordings, or other user generated-content,

non-public communications, and information regarding an individual's interaction with an internet website, mobile application, or advertisement;

(vi) historical or real-time geolocation data;

(vii) audio, electronic, visual, thermal, olfactory, or similar information;

(viii) education records, as defined in section thirty-three hundred two of the education law;

(ix) political information or information on criminal convictions or arrests;

(x) any required security code, access code, password, or username necessary to permit access to the account of an individual;

(xi) characteristics of protected classes under the human rights law, including race, color, national origin, religion, sex, age, or disability; or

(xii) an inference drawn from any of the information described in this paragraph to create a profile about an individual reflecting the individual's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, or aptitudes.

(b) The term personal data does not include publicly available information. "Publicly available information":

(i) means information that is lawfully made available from federal, state, or local government records; and

(ii) does not include biometric information collected by a covered entity about an individual without the individual's knowledge, or information used for a purpose that is not compatible with the purpose for which the information is maintained and made available in government records.

(c) Personal data does not include de-identified data.

11. "Process" or "processing" means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, deletion, or destruction.

12. "Processor" means a natural or legal person who processes personal data on behalf of the controller.

13. "Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

14. "Restriction of processing" means the marking of stored personal data with the aim of limiting the processing of such personal data in the future.

15.(a) "Sale", "sell" or "sold" means the exchange of personal data for consideration by the controller to a third party.

(b) "Sale" does not include the following: (i) the disclosure of personal data to a processor who processes the personal data on behalf of the controller; (ii) the disclosure of personal data to a third party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer or otherwise in a manner that is consistent with a consumer's reasonable expectations

considering the context in which the consumer provided the personal data to the controller; (iii) the disclosure or transfer of personal data to an affiliate of the controller; or (iv) 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, if consumers are notified of the transfer of their data and of their rights under this article and affirmatively consent to the disclosure and transfer of data.

16. "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred over time from a consumer's activities across web sites, applications or online services. It does not include advertising to a consumer based upon the consumer's current visit to a web site, application, or online service, or in response to the consumer's request for information or feedback.

17. "Opt-in" means affirmative, express consent of an individual for a covered entity to use, disclose, or permit access to the individual's personal data after the individual has received explicit notification of the request of the covered entity with respect to that data.

§ 1101. Jurisdictional scope. 1. This article applies to legal entities that conduct business in New York state or produce products or services that are intentionally targeted to residents of New York state.

2. This article does not apply to:

(a) state and local governments;

(b) personal data sets to the extent that they are regulated by the federal health insurance portability and accountability act of 1996, the federal health information technology for economic and clinical health act, or the Gramm-Leach-Bliley act of 1999; or

(c) data sets maintained for employment records purposes.

§ 1102. Data fiduciary. 1. Personal data of consumers shall not be used, processed or transferred to a third party, unless the consumer provides express and documented consent. Every legal entity, or any affiliate of such entity, and every controller and data broker, which collects, sells or licenses personal information of consumers, shall exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk; and shall act in the best interests of the consumer, without regard to the interests of the entity, controller or data broker, in a manner expected by a reasonable consumer under the circumstances.

(a) Every legal entity, or affiliate of such entity, and every controller and data broker to which this article applies shall:

(i) reasonably secure personal data from unauthorized access; and

(ii) promptly inform a consumer of any breach of the duty described in this paragraph with respect to personal data of such consumer.

(b) A legal entity, an affiliate of such entity, controller or data broker may not use personal data, or data derived from personal data, in any way that:

(i) will benefit the online service provider to the detriment of an end user; and

(ii) (A) will result in reasonably foreseeable and material physical or financial harm to a consumer; or

(B) would be unexpected and highly offensive to a reasonable consumer.

(c) A legal entity, or affiliate of such entity, controller or data broker:

(i) may not disclose or sell personal data to, or share personal data with, any other person except as consistent with the duties of care and loyalty under paragraphs (a) and (b) of this subdivision;

(ii) may not disclose or sell personal data to, or share personal data with, any other person unless that person enters into a contract that imposes the same duties of care, loyalty, and confidentially toward the consumer as are imposed under this section; and

(iii) shall take reasonable steps to ensure that the practices of any person to whom the entity, or affiliate of such entity, controller or data broker discloses or sells, or with whom the entity, or affiliate of such entity, controller or data broker shares. Personal data fulfills the duties of care, loyalty, and confidentiality assumed by the person under the contract described in subparagraph (ii) of this paragraph, including by auditing, on a regular basis, the data security and data information practices of any such entity, or affiliate of such entity, controller or data broker.

2. For the purposes of this section the term "privacy risk" means potential adverse consequences to consumers and society arising from the processing of personal data, including, but not limited to:

(a) direct or indirect financial loss or economic harm;

(b) physical harm;

(c) psychological harm, including anxiety, embarrassment, fear, and other demonstrable mental trauma;

(d) significant inconvenience or expenditure of time;

(e) adverse outcomes or decisions with respect to an individual's eligibility for rights, benefits or privileges in employment (including, but not limited to, hiring, firing, promotion, demotion, compensation), credit and insurance (including, but not limited to, denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services;

(f) stigmatization or reputational harm;

(g) disruption and intrusion from unwanted commercial communications or contacts;

(h) price discrimination;

(i) effects on an individual that are not reasonably foreseeable, contemplated by, or expected by the individual to whom the personal data relates, that are nevertheless reasonably foreseeable, contemplated by, or expected by the controller assessing privacy risk, that:

(A) alters that individual's experiences;

(B) limits that individual's choices;

(C) influences that individual's responses; or

(D) predetermines results; or

(j) other adverse consequences that affect an individual's private life, including private family matters, actions and communications within an individual's home or similar physical, online, or digital location, where an individual has a reasonable expectation that personal data will not be collected or used.

3. The fiduciary duty owed to a consumer under this section shall supersede any duty owed to owners or shareholders of a legal entity or affiliate thereof, controller or data broker, to whom this article apples.

§ 1103. Consumer rights. Any entity subject to the provisions of this article shall provide notice to consumers of their rights under this article and shall provide consumers the opportunity to opt in or opt out of processing their personal data in such a manner that the consumer

must select and clearly indicate their consent or denial of consent. Controllers shall facilitate requests to exercise the consumer rights set forth in subdivisions one through six of this section. 1. On request from a consumer, a controller shall confirm whether or not personal data concerning the consumer is being processed by the controller, including whether such personal data is sold to data brokers, and, where personal data concerning the consumer is being processed by the controller, provide access to such personal data concerning the consumer and the names of third parties to whom personal data is sold or licensed. On request from a consumer, a controller shall provide a copy of the personal data undergoing processing free of charge, up to twice annually. For any further copies requested by the consumer, the controller may charge a reasonable fee based on administrative costs. Where the consumer makes the request by electronic means, and unless otherwise requested by the consumer, the information shall be provided in a commonly used electronic form.

2. On request from a consumer, the controller, without undue delay, shall correct inaccurate personal data concerning the consumer. Taking into account the purposes of the processing, the controller shall complete incomplete personal data, including by means of providing a supplementary statement.

3. (a) On request from a consumer, a controller shall delete the consumer's personal data without undue delay where one of the following grounds applies:

(i) The personal data is no longer necessary in relation to the purposes for which the personal data was collected or otherwise processed;

(ii) For processing that requires consent under section eleven hundred five of this article, the consumer withdraws consent to processing;

(iii) The personal data has been unlawfully processed;

(iv) To comply with a legal obligation under federal, state, or local law to which the controller is subject; or

(v) The consumer otherwise requests that the data be deleted.

(b) Where the controller is obliged to delete personal data under this section that has been disclosed to third parties by the controller, including data brokers that received the data through a sale, the controller shall take reasonable steps, which may include technical measures, to inform other controllers that are processing the personal data that the consumer has requested the deletion by the other controllers of any links to, or copy or replication of, the personal data. Compliance with this obligation shall take into account available technology and cost of implementation.

(c) This subdivision does not apply to the extent processing is necessary:

(i) for exercising the right of free speech;

(ii) for compliance with a legal obligation that requires processing by federal, state, or local law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(iii) for reasons of public interest in the area of public health, where the processing (A) is subject to suitable and specific measures to safeguard the rights of the consumer; and (B) is processed by or under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law;

(iv) for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, where the

deletion of such personal data is likely to render impossible or seriously impair the achievement of the objectives of the processing; or

(v) for the establishment, exercise, or defense of legal claims.

4. (a) The controller shall cease processing if one of the following grounds applies:

(i) The accuracy of the personal data is contested by the consumer, for a period enabling the controller to verify the accuracy of the personal data;

(ii) The processing is unlawful and the consumer opposes the deletion of the personal data and requests the restriction of processing instead;

(iii) The controller no longer needs the personal data for the purposes of the processing, but such personal data is required by the consumer for the establishment, exercise, or defense of legal claims; or

(iv) The consumer otherwise requests that the controller cease processing.

(b) Where personal data is subject to a restriction or processing under this subdivision, the personal data shall, with the exception of storage, only be processed (i) with the consumer's consent; (ii) for the establishment, exercise, or defense of legal claims; or (iii) for reasons of important public interest under federal, state, or local law.

(c) Where a consumer has taken steps by the online selection of options related to sharing personal data a controller is obligated to adhere to such selections.

5. (a) On request from a consumer, the controller shall provide the consumer any personal data concerning such consumer that such consumer has provided to the controller in a structured, commonly used, and machine-readable format if (i)(A) the processing of such personal data requires consent under section eleven hundred five of this article, (B) the processing of such personal data is necessary for the performance of a contract to which the consumer is a party, or (C) in order to take steps at the request of the consumer prior to entering into a contract; and (ii) the processing is carried out by automated means.

(b) Controllers shall transmit the personal data requested under this subdivision directly from one controller to another, where technically feasible, and transmit the personal data to another controller without hindrance from the controller to which the personal data was provided.

(c) Requests for personnel data under this subdivision shall be without prejudice to subdivision three of this section.

(d) The rights provided in this subdivision do not apply to processing necessary for the performance of a task carried out in the public interest and shall not adversely affect the rights of consumers.

6. A consumer shall not be subject to a decision based solely on profiling which produces legal effects concerning such consumer or similarly significantly affects the consumer. Legal or similarly significant effects include, but are not limited to, denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, and health care services.

(a) This subdivision does not apply if the decision is authorized by federal or state law to which the controller is subject and which incorporates suitable measures to safeguard the consumer's rights and legitimate interests, as indicated by the risk assessments required by section eleven hundred five of this article.

(b) Notwithstanding paragraph (a) of this subdivision, the controller shall implement suitable measures to safeguard consumer's rights and legitimate interests with respect to decisions based solely on profil-

ing, including providing human review of the decision, to express the consumer's point of view with respect to the decision, and to contest the decision.

7. A controller shall communicate any correction, deletion, or restriction of processing carried out in accordance with subdivisions two, three or four of this section to each third-party recipient to whom the personal data has been disclosed, including third parties that received the data through a sale, unless this proves impossible. The controller shall inform the consumer about such third-party recipients, if any, if the consumer requests such information.

8. A controller shall provide information on action taken on a request under subdivisions one through six of this section without undue delay and in any event within thirty days of receipt of the request. That period may be extended by sixty additional days where necessary, taking into account the complexity and number of the requests. The controller shall inform the consumer of any such extension within thirty days of receipt of the request, together with the reasons for the delay. Where the consumer makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the consumer.

(a) If a controller does not take action on the request of a consumer, the controller shall inform the consumer without undue delay and at the latest within thirty days of receipt of the request of the reasons for not taking action and any possibility for internal review of the decision by the controller.

(b) Information provided under this section must be provided by the controller free of charge to the consumer. Where requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (i) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (ii) refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

(c) Where the controller has reasonable doubts concerning the identity of the consumer making a request under subdivisions one through six of this section, the controller may request the provision of additional information necessary to confirm the identity of the consumer.

(d) A controller shall conduct an internal review on any action taken upon request of a consumer under subdivisions one through six of this section.

§ 1104. Transparency. 1. Controllers shall be transparent and accountable for their processing of personal data, by making available in a form that is reasonably accessible to consumers a clear, meaningful privacy notice that is easily understood and which includes:

(a) the categories of personal data collected by the controller;

(b) the purposes for which the categories of personal data is used and disclosed to third parties, if any;

(c) the rights that consumers may exercise pursuant to section eleven hundred three of this article, if any;

(d) the categories of personal data that the controller shares with third parties, if any; and

(e) the names and categories of third parties, if any, with whom the controller shares personal data.

2. Controllers that engage in profiling shall disclose such profiling to the consumer at or before the time personal data is obtained, includ-

ing meaningful information about the logic involved and the significance and envisaged consequences of the profiling.

3. If a controller sells personal data to data brokers or processes personal data for direct marketing purposes, including targeted marketing and profiling to the extent that it is related to such direct marketing, it shall disclose such processing, as well as the manner in which a consumer may exercise the right to object to such processing, in a clear and prominent manner.

§ 1105. Responsibility according to role. 1. Controllers and brokers shall be responsible for meeting the obligations set forth under this article.

2. Processors and brokers are responsible under this article for adhering to the instructions of the controller and assisting the controller to meet its obligations under this article.

3. Processing by a processor shall be governed by a contract between the controller and the processor that is binding on the processor and that sets out the processing instructions to which the processor is bound.

§ 1106. De-identified data. A controller or processor that uses de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the de-identified data is subject, and shall take appropriate steps to address any breaches of contractual commitments.

§ 1107. Exemptions. 1. The obligations imposed on controllers or processors under this article do not restrict a controller's or processor's ability to:

(a) comply with federal, state, or local laws;

(b) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

(c) disclose personal data to a law enforcement agency if such information:

(i) was inadvertently obtained by the controller or data broker; and

(ii) appears to pertain to the commission of a crime;

(d) cooperate with a governmental entity if the controller or data broker, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure of personal data without delay;

(e) investigate, exercise, or defend legal claims; or

(f) prevent or detect identity theft, fraud, or other criminal activity or verify identities.

2. The obligations imposed on controllers or processors under this article do not apply where compliance by the controller or processor with this article would violate an evidentiary privilege under New York law and do not prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under New York law as part of a privileged communication.

3. A controller or processor that discloses personal data to a third-party controller or processor in compliance with the requirements of this article is not in violation of this article, including under section eleven hundred eight of this article, if the third-party recipient processes such personal data in violation of this article, provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the third-party recipient intended to commit a violation. A third-party recipient receiving personal data from a controller or processor is likewise not

liable under this article, including under section eleven hundred eight of this article, for the obligations of a controller or processor to whom it provides services.

4. This article does not require a controller or processor to do the following:

(a) re-identify de-identified data;

(b) retain personal data concerning a consumer that he or she would not otherwise retain in the ordinary course of business; or

(c) comply with a request to exercise any of the rights under subdivisions one through six of section eleven hundred three of this article if the controller is unable to verify, using commercially reasonable efforts, the identity of the consumer making the request.

5. Obligations imposed on controllers and processors under this article do not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

§ 1108. Liability. Where more than one controller or processor, or both a controller and a processor, involved in the same processing, is in violation of this article, the liability shall be allocated among the parties according to principles of comparative fault, unless such liability is otherwise allocated by contract among the parties.

§ 1109. Enforcement. 1. The legislature finds that the practices covered by this article are matters vitally affecting the public interest for the purpose of providing consumer protection from deceptive acts and practices under article twenty-two-A of this chapter. A violation of this article is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying article twenty-two-A of this chapter.

2. The attorney general may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce this article.

3. In addition to any right of action granted to any governmental body pursuant to this section, any person who has been injured by reason of a violation of this article may bring an action in his or her own name to enjoin such unlawful act, or to recover his or her actual damages, or both such actions. The court may award reasonable attorney's fees to a prevailing plaintiff.

4. Any controller or processor who violates this article is subject to an injunction and liable for damages and a civil penalty. When calculating damages and civil penalties, the court shall consider the number of affected individuals, the severity of the violation, and the size and revenues of the covered entity. Each individual whose information was unlawfully processed counts as a separate violation. Each provision of this article that was violated counts as a separate violation.

§ 1110. Preemption. This article supersedes and preempts laws adopted by any local entity regarding the processing of personal data by controllers or processors.

§ 3. This act shall take effect on the one hundred eightieth day after it shall have become a law.