STATE OF NEW YORK

974--A

2025-2026 Regular Sessions

IN ASSEMBLY

(Prefiled)

January 8, 2025

Introduced by M. of A. ROZIC, HEVESI, BICHOTTE HERMELYN, BEEPHAN, WOERNER, LEE, TORRES, SIMONE -- read once and referred to the Committee on Consumer Affairs and Protection -- reported and referred to the Committee on Codes -- recommitted to the Committee on Codes in accordance with Assembly Rule 3, sec. 2 -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

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 shall be known and may be cited as the "New York data protection act".

§ 2. Legislative intent. 1. Privacy is a fundamental right and an essential element of freedom. Advances in technology have produced rampant growth in the amount and categories of personal data being generated, collected, stored, analyzed, and potentially shared, which presents both promise and peril. Companies collect, use and share our personal data in ways that can be difficult for ordinary consumers to understand. Opaque data processing policies make it impossible to evaluate risks and compare privacy-related protections across services, stifling competition. Algorithms quietly make decisions with critical consequences for New York consumers, often with no human accountability. Behavioral advertising generates profits by turning people into products and their activity into assets. New York consumers deserve more notice and more control over their data and their digital privacy.

2. This act seeks to help New York consumers regain their privacy. It gives New York consumers the ability to exercise more control over their personal data and requires businesses to be responsible, thoughtful, and accountable managers of that information. To achieve this, this act

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

LBD02963-03-6

provides New York consumers a number of new rights, including clear notice of how their data is being used, processed and shared; the ability to access and obtain a copy of their data in a commonly used electronic format, with the ability to transfer it between services; and the ability to correct inaccurate data and to delete their data. This act also imposes obligations upon businesses to maintain reasonable data security for personal data, to notify New York consumers of foreseeable harms arising from use of their data and to obtain specific consent for that use, and to conduct regular assessments to ensure that data is not being used for unacceptable purposes. These data assessments can be obtained and evaluated by the New York State Attorney General, who is empowered to obtain penalties for violations of this act and prevent future violations.

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

ARTICLE 42-A

NEW YORK DATA PROTECTION ACT

§ 1200. Definitions. The following definitions apply for the purposes of this article unless the context clearly requires otherwise:

1. "Biometric information" means any measurable physical, physiological, or behavioral characteristic that is attributable to a person, including, but not limited to facial characteristics, fingerprint characteristics, hand characteristics, eye characteristics, vocal characteristics, and any other characteristics that can be used to identify a person including, but not limited to: fingerprints; handprints; retina and iris patterns; DNA sequence; voice; gait; and facial geometry. "Biometric information" 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, unless such data is generated to identify a specific individual.

2. "Business associate" has the same meaning as in Title 45 of the C.F.R., established pursuant to the federal Health Insurance Portability and Accountability Act of 1996.

3. "Consent" means a clear affirmative act signifying a freely given, specific, informed, and unambiguous indication of a consumer's agreement to the processing of data relating to the consumer. Consent may be withdrawn at any time, and a controller must provide clear, conspicuous, and consumer-friendly means to withdraw consent. The burden of establishing consent is on the controller. Consent does not include: (a) an agreement of general terms of use or a similar document that references unrelated information in addition to personal data processing; (b) an agreement obtained through fraud, deceit or deception; (c) any act that does not constitute a user's intent to interact with another party such as hovering over, pausing or closing any content; or (d) a pre-checked box or similar default.

4. "Consumer" means a natural person who is a New York resident acting only in an individual or household context. It does not include a natural person known to be acting in a professional or employment context.

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

6. "Covered entity" has the same meaning as in Title 45 of the C.F.R., established pursuant to the federal Health Insurance Portability and Accountability Act of 1996.

7. "Decisions that produce legal or similarly significant effects" means decisions made by the 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.

8. "Deidentified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to an identified or identifiable particular consumer, household, or device, provided that the processor or controller that processes the data:

(a) implements reasonable technical safeguards to ensure that the data cannot be associated with a consumer, household or device;

(b) publicly commits to process the data only as deidentified data and not attempt to reidentify the data, except that the controller or processor may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision;

(c) contractually obligates any recipients of the deidentified data to comply with all provisions of this article; and

(d) any deidentified data not otherwise exempt under this article, once subsequently reidentified shall not be considered deidentified.

9. "Device" means any physical object that is capable of connecting to the internet, directly or indirectly, or to another device and is intended for use by a natural person or household or, if used outside the home, for use by the general public.

10. "Household" means a group, however identified, of consumers who cohabitate with one another at the same residential address and may share use of common devices or services.

11. "Identified or identifiable" means a natural person who can be identified, directly or indirectly, such as by reference to an identifier such as a name, an identification number, precise geolocation data, or an online or device identifier.

12. "Person" means a natural person or a legal entity, including but not limited to a proprietorship, partnership, limited partnership, corporation, company, limited liability company or corporation, association, or other firm or similar body, or any unit, division, agency, department, or similar subdivision thereof.

13. "Personal data" means any data that identifies or could reasonably be linked, directly or indirectly, with a specific natural person, or household. "Personal data" does not include deidentified data, information that is lawfully made publicly available from federal, state or local government records, or information that a controller has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media.

14. "Precise geolocation data" means information derived from technology, including, but not limited to, global position system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of one thousand seven hundred fifty feet, except as prescribed by regulations. Precise geolocation data does not include the content of communications or any data generated by or

connected to advance utility metering infrastructure systems or equipment for use by a utility.

15. "Process", "processes" or "processing" means an operation or set of operations which are performed on data or on sets of data, including but not limited to the collection, use, access, sharing, monetization, analysis, retention, creation, generation, derivation, recording, organization, structuring, storage, disclosure, transmission, analysis, disposal, licensing, destruction, deletion, modification, or deidentification of data.

16. "Processor" means a person that processes personal data on behalf of the controller.

17. "Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. Profiling does not include evaluation, analysis, or prediction based solely upon a natural person's current search query or activities on, or current visit to, the controller's website or online application.

18. "Sale", "sell", or "sold" means the disclosure, transfer, conveyance, sharing, licensing, making available, processing, granting of permission or authorization to process, or other exchange of personal data, or providing access to personal data for monetary or other valuable consideration by the controller to a third party. "Sale" does not include the following:

(a) the disclosure of data to a processor who processes the data on behalf of the controller and which is contractually prohibited from using it for any purpose other than as instructed by the controller;

(b) the disclosure or transfer of data as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which another entity assumes control or ownership of all or a majority of the controller's assets; or

(c) the disclosure of personal data to a third party necessary for purposes of providing a product, service, or interaction with such third party, when the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party; or

(d) the disclosure or transfer of personal data to an affiliate of the controller under the same branding:

19. "Sensitive data" means personal data that reveals:

(a) racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, gender identity or citizenship or immigration status;

(b) biometric information for the purpose of uniquely identifying a natural person;

(c) precise geolocation data; or

(d) social security, financial account, passport or driver's license numbers.

20. "Targeted advertising" means advertising based upon profiling. It does not include recommendations by a controller to a consumer with whom the controller has an existing relationship that are made on the controller's websites or online applications and are based solely upon personal data that the controller has collected from the consumer on such websites or online applications regarding content, products, or services provided by the controller.

21. "Third party" means, with respect to a particular interaction or occurrence, a person, public authority, agency, or body other than the consumer, the controller, or processor of the controller. A third party may also be a controller if the third party, alone or jointly with others, determines the purposes and means of the processing of personal data.

22. "Verifiable" means to use reasonable means to determine that a request to exercise any of the rights afforded in this act is being made by, or on behalf of, the individual who is entitled to exercise such rights authorized by this article; provided that any additional personal information a controller requests for the purpose of verification must be strictly necessary for the purpose of confirming the identity of such individual and shall not be processed or used for any purpose other than verifying the identity of the individual and shall be deleted immediately upon verification or failure to verify the individual. Such verification shall not extend the maximum allowable time within which the regulated entity may satisfy a request by a consumer.

§ 1201. Jurisdictional scope. 1. This article applies to legal persons that conduct business in New York or produce products or services that are targeted to residents of New York, and satisfy one or more of the following thresholds:

(a) have annual gross revenue of twenty-five million dollars or more;

(b) controls or processes personal data of one hundred thousand consumers or more; or

(c) derives over fifty percent of gross revenue from the sale of personal data.

2. This article does not apply to:

(a) local, state, or federal governments and their agencies, authorities or public corporations as defined in section sixty-six of the general construction law or data processed by or on behalf of such governmental entities provided that the data is only processed for governmental purposes;

(b) a national securities association registered pursuant to section 15A of the Securities Exchange Act of 1934, as amended, or regulations adopted thereunder or a registered futures association so designated pursuant to section 17 of the Commodity Exchange Act, as amended, or any regulations adopted thereunder;

(c) any nonprofit entity identified in section four hundred five of the financial services law to the extent such organization collects, processes, uses, or shares data solely in relation to identifying, investigating, or assisting (i) law enforcement agencies in connection with suspected insurance-related criminal or fraudulent acts; or (ii) first responders in connection with catastrophic events;

(d) information that meets the following criteria:

(i) personal data collected, processed, or disclosed pursuant to and in compliance with the federal Gramm-Leach-Bliley act (P.L. 106-102), and implementing regulations;

(ii) personal data collected, processed, or disclosed pursuant to the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.), if the collection, processing, sale, or disclosure is in compliance with that law;

(iii) personal data regulated by the federal Family Educational Rights and Privacy Act, U.S.C. Sec. 1232g and its implementing regulations;

(iv) personal data collected, processed, or disclosed pursuant to the federal Farm Credit Act of 1971 (as amended in 12 U.S.C. Sec. 2001-2279cc) and its implementing regulations (12 C.F.R. Part 600 et

seq.) if the collection, processing, sale, or disclosure is in compliance with that law;

(v) personal data regulated by section two-d of the education law;

(vi) data processed or maintained (A) 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, (B) as the emergency contact information of an individual under this section used for emergency contact purposes, or (C) that is necessary to retain to administer benefits for another individual relating to an individual under clause (A) of this subparagraph and used for the purposes of administering such benefits;

(vii) information maintained by a financial institution that is subject to the Gramm-Leach-Bliley Act (Public Law 106-103), to the extent the financial institution maintains the information in the same manner as personal data as described in subparagraph (i) of this paragraph;

(viii) personal data processed only for one or more of the following purposes:

(A) product registration and tracking consistent with applicable United States Food and Drug Administration regulations and guidance;

(B) public health activities and purposes as described in Section 164.512 of Title 45 of the Code of Federal Regulations; and/or

(C) activities related to quality, safety, or effectiveness regulated by the United States Food and Drug Administration; or

(ix) personal data collected, processed, or disclosed pursuant to and in compliance with any opt-out program authorized by the public service commission or any other opt-out community distributed generation programs authorized in law; or

(e) (i) an activity involving the collection, maintenance, disclosure, communication, or use of any personal data 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, as defined in Title 15 U.S.C. Sec. 1681a(f), by a furnisher of information, as set forth in Title 15 U.S.C. Sec. 1681s-2, who provides information for use in a consumer report, as defined in Title 15 U.S.C. Sec. 1861a(d), and by a user of a consumer report, as set forth in Title 15 U.S.C. Sec. 1681b.; and

(ii) this paragraph shall apply only to the extent that such activity involving the collection, maintenance, disclosure, communication, or use of such data by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act, Title 15 U.S.C. Sec. 1681 et seq., and the data is not collected, maintained, used, communicated, disclosed, or sold except as authorized by the Fair Credit Reporting Act.

§ 1202. Consumer rights. 1. Right to notice. (a) Notice. Each controller that processes a consumer's personal data must make publicly and consistently available, in a conspicuous and readily accessible manner, a notice containing the following:

(i) a description of the consumer's rights under subdivisions two through seven of this section and how a consumer may exercise those rights, including how to withdraw consent;

(ii) the categories of personal data processed by the controller and by any processor who processes personal data on behalf of the controller;

(iii) the sources from which personal data is collected;

(iv) the purposes for processing personal data;

(v) the categories of third parties to whom the controller disclosed, shared, transferred or sold personal data and, for each category of third party, (A) the categories of personal data being shared, disclosed, transferred, or sold to the third party, (B) the purposes for which personal data is being shared, disclosed, transferred, or sold to the third party, (C) any applicable retention periods for each category of personal data processed by the third parties or processed on their behalf, or if that is not possible, the criteria used to determine the period, and (D) whether the third parties may use the personal data for targeted advertising; and

(vi) the controller's retention period for each category of personal data that they process or is processed on their behalf, or if that is not possible, the criteria used to determine that period.

(b) Notice requirements.

(i) The notice must be written in plain language and in no less than twelve point font and consistent with section two hundred two-a of the executive law.

(ii) The categories of personal data processed and purposes for which each category of personal data is processed must be described in a clear and conspicuous manner, at a level specific enough to enable a consumer to exercise meaningful control over their personal data but not so specific as to render the notice unhelpful to a consumer.

(iii) The notice must be dated with its effective date and updated at least annually. When the information required to be disclosed to a consumer pursuant to paragraph (a) of this subdivision has not changed since the immediately previous notice (whether initial, annual, or revised) provided to the consumer, a controller may issue a statement that no changes have been made.

(iv) The notice, as well as each version of the notice in effect in the preceding six years, must be easily accessible to consumers and capable of being viewed by consumers at any time.

2. Right to opt out. (a) A controller must allow consumers the right to opt out, at any time, of processing personal data concerning the consumer for the purposes of:

(i) targeted advertising;

(ii) the sale of personal data; and

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

(b) A controller must provide clear and conspicuous means for the consumer or their agent to opt out of processing and clearly present as the most conspicuous choice an option to simultaneously opt out of all processing purposes set forth in paragraph (a) of this subdivision.

(c) A controller must not process personal data for any purpose from which the consumer has opted out.

(d) If a consumer has opted out of the processing of personal data pursuant to paragraph (a) of this subdivision, a controller must not request that the consumer opt back in to such processing in a way that is manifestly excessive or unduly burdensome to the consumer, and in no event shall make such a request to the consumer more than twice annually.

(e) Controllers must treat user-enabled privacy controls in a browser, browser plug-in, smartphone application, operating system, device setting, or other mechanism that communicates or signals the consumer's choice to opt out of the processing of personal data in furtherance of targeted advertising, or the sale of their personal data as an opt out

under this article. To the extent that the privacy control conflicts with a consumer's consent, the controller shall comply with the privacy control but may notify the consumer of such conflict and provide to such consumer the choice to give controller specific consent to such processing.

(f) The attorney general shall publish a list of user-enabled controls that controllers must recognize on its website with enough technical information to allow controllers and processors to recognize such controls.

3. Sensitive data. (a) A controller must obtain freely given, specific, informed, and unambiguous opt-in verifiable consent from a consumer to:

(i) process the consumer's sensitive data related to that consumer for any purpose other than those in subdivision two of section twelve hundred four of this article; or

(ii) make any changes to the existing processing or processing purpose, including those regarding the method and scope of collection, of the consumer's sensitive data that may be less protective of the consumer's sensitive data than the processing to which the consumer has previously given their freely given, specific, informed, and unambiguous opt-in consent.

(b) Any request for consent to process sensitive data must be provided to the consumer, prior to processing their sensitive data, in a standalone disclosure that is separate and apart from any contract or privacy policy. The request for consent must:

(i) be written in a twelve point font or greater and include a clear and conspicuous description of each category of data and processing purpose for which consent is sought;

(ii) clearly identify and distinguish between categories of data and processing purposes that are necessary to provide the services or goods requested by the consumer and categories of data and processing purposes that are not necessary to provide the services or goods requested by the consumer;

(iii) enable a reasonable consumer to easily identify the categories of data and processing purposes for which consent is sought;

(iv) clearly present as the most conspicuous choice an option to provide only the consent necessary to provide the services or goods requested by the consumer;

(v) clearly present an option to deny consent; and

(vi) where the request seeks consent to sharing, disclosure, transfer, or sale of sensitive data to third parties, identify the categories of such third parties, the categories of data sold or shared with them, the processing purposes, the retention period, or if that is not possible, the criteria used to determine the period, and state if such sharing, disclosure, transfer, or sale enables or involves targeted advertising. The details of the categories of such third parties, and the categories of data, processing purposes, and the retention period, may be set forth in a different disclosure, provided that the request for consent contains a conspicuous and directly accessible link to that disclosure.

(c) Targeted advertising and sale of personal data shall not be considered processing purposes that are necessary to provide services or goods requested by a consumer.

(d) Once a consumer has provided freely given, specific, informed, and unambiguous opt-in consent to process their sensitive data for a processing purpose, a controller may rely on such consent until it is withdrawn.

(e) A controller must provide a mechanism for a consumer to withdraw previously given consent at any time. Such mechanism shall make it as easy for a consumer to withdraw their consent as it is for such consumer to provide consent.

(f) A controller must not infer that a consumer has provided freely given, specific, informed, and unambiguous opt-in consent from the consumer's inaction or the consumer's continued use of a service or product provided by the controller.

(g) Controllers must not request consent from a consumer who has previously withheld or denied consent to process sensitive data, until at least twelve months after a denial, unless consent is necessary to provide the services or goods requested by the consumer.

(h) Controllers must treat user-enabled privacy controllers in a browser, browser plug-in, smartphone application, operating system, device setting, or other mechanism that communicates or signals the consumer's choices to opt out of the processing of personal data in furtherance of targeted advertising, the sale of their personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer as a denial of consent to process sensitive data under this article. To the extent that the privacy control conflicts with a consumer's consent, the privacy control settings govern, unless the consumer provides freely given, specific, informed, and unambiguous opt-in consent to override the privacy control, however, the controller may notify such consumer of such conflict and provide to the consumer the choice to give controller-specific consent to such processing.

(i) A controller must not discriminate against a consumer for exercising their rights under this article or withholding or denying consent, including, but not limited to, by:

(i) denying services or goods to the consumer, unless the consumer does not consent to processing necessary to provide the services or goods requested by the consumer;

(ii) charging different prices for goods or services, including through the use of discounts or other benefits, imposing penalties, or providing a different level or quality of services or goods to the consumer; or

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

(j) In the event of a merger, acquisition, bankruptcy, or other transaction in which another entity assumes control or ownership of all or majority of the controller's assets, any consent provided to the controller by a consumer relating to sensitive data prior to such transaction other than consent to processing necessary to provide services or goods requested by the consumer, shall be deemed withdrawn.

4. Right to access. Upon the verifiable request of a consumer, a controller shall:

(a) confirm whether or not the controller is processing or has processed personal data of that consumer, and provide access to a copy of any such personal data in a manner understandable to a reasonable consumer when requested; and

(b) provide the category of each processor or third party to whom the controller disclosed, transferred, or sold the consumer's personal data and, for each category of processor or third party, (i) the categories of the consumer's personal data disclosed, transferred, or sold to each processor or third party and (ii) the purposes for which each category

of the consumer's personal data was disclosed, transferred, or sold to each processor or third party.

5. Right to portable data. Upon a verifiable request, and to the extent technically feasible, the controller must provide to the consumer a copy of all of, or a portion of, as designated in a verifiable request, the consumer's personal data in a structured, commonly used and machine-readable format that allows the consumer to transmit the data to another person of the consumer's or their agent's designation without hindrance.

6. Right to correct. (a) Upon the verifiable request of a consumer or their agent, a controller must conduct a reasonable investigation to determine whether personal data, the accuracy of which is disputed by the consumer, is inaccurate, with such investigation to be concluded within the time period set forth in paragraph (a) of subdivision eight of this section.

(b) Notwithstanding paragraph (a) of this subdivision, a controller may terminate an investigation initiated pursuant to such paragraph if the controller reasonably and in good faith determines that the dispute by the consumer is wholly without merit, including by reason of a failure by a consumer to provide sufficient information to investigate the disputed personal data. Upon making any determination in accordance with this paragraph that a dispute is wholly without merit, a controller must, within the time period set forth in paragraph (a) of subdivision eight of this section, provide the affected consumer a statement in writing that includes, at a minimum, the specific reasons for the determination, and identification of any information required to investigate the disputed personal data, which may consist of a standardized form describing the general nature of such information.

(c) If, after any investigation under paragraph (a) of this subdivision of any personal data disputed by a consumer, an item of the personal data is found to be inaccurate or incomplete, or cannot be verified, the controller must:

(i) correct the inaccurate or incomplete personal data of the consumer; and

(ii) unless it proves impossible or involves disproportionate effort, communicate such request to each third party to whom the controller disclosed, transferred, or sold the personal data within one year preceding the consumer's request, and to require those third parties to do the same for any further third parties they disclosed, transferred, or sold the personal data to.

(d) If the investigation does not resolve the dispute, the consumer may file with the controller a brief statement setting forth the nature of the dispute. Whenever a statement of a dispute is filed, unless there exists reasonable grounds to believe that it is wholly without merit, the controller must note that it is disputed by the consumer and include either the consumer's statement or a clear and accurate codification or summary thereof with the disputed personal data whenever it is disclosed, transferred, or sold to any processor or third party.

7. Right to delete. (a) Upon the verifiable request of a consumer, a controller must:

(i) within thirty days after receiving the verifiable request, delete any or all of the consumer's personal data, as directed by the consumer or their agent, that the controller possesses or controls; and

(ii) unless it proves impossible or involves disproportionate effort that is documented in writing by the controller, communicate such request to each third party to whom the controller disclosed, trans-

ferred or sold the personal data within one year preceding the consumer's request and to require those third parties to do the same for any further third parties they disclosed, transferred, or sold the personal data to.

(b) For personal data that is not possessed by the controller but by a processor of the controller, the controller may choose to (i) communicate the consumer's request for deletion to the processor, or (ii) request that the processor return to the controller the personal data that is the subject of the consumer's request and delete such personal data upon receipt of the request.

(c) A consumer's deletion of their online account must be treated as a request to the controller to delete all of that consumer's personal data directly related to that account.

(d) A controller must maintain reasonable procedures designed to prevent the reappearance in its systems, and in any data it discloses, transfers, or sells to any third party, the personal data that is deleted pursuant to this subdivision.

(e) A controller is not required to comply with a consumer's request to delete personal data if:

(i) complying with the request would prevent the controller from performing accounting functions, processing refunds, effectuating a product recall pursuant to federal or state law, or fulfilling warranty claims, provided that the personal data that is the subject of the request is not processed for any purpose other than such specific activities; or

(ii) it is necessary for the controller to maintain the consumer's personal data to engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the controller's deletion of the information is likely to render impossible or seriously impair the achievement of such research, provided that the consumer has given informed consent and the personal data is not processed for any purpose other than such research.

(f) Where a consumer's request for deletion is denied, the controller shall provide the consumer with a written justification for such denial.

8. Responding to requests. (a) A controller must take action under subdivisions four through seven of this section and inform the consumer of any actions taken without undue delay and in any event within thirty days of receipt of the request. That period may be extended once by thirty additional days where reasonably necessary, taking into account the complexity and number of the requests. The controller must inform the consumer of any such extension within thirty days of receipt of the request, together with the reasons for the delay. When a controller denies any such request, it must within this period disclose to the consumer a statement in writing of the specific reasons for the denial and instructions for how to appeal the decision.

(b) A controller shall permit the exercise of rights and carry out its obligations set forth in subdivisions four through seven of this section free of charge, at least twice annually 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 to cover the administrative costs of complying with the request or (ii) refuse to act on the request and notify the consumer of the reason for refusing the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

(c) (i) A controller shall promptly attempt, using commercially reasonable efforts, to verify that all requests to exercise any rights set forth in any section of this article requiring a verified request were made by the consumer who is the subject of the data, or by a person lawfully exercising the right on behalf of the consumer who is the subject of the data. Commercially reasonable efforts shall be determined based on the totality of the circumstances, including the nature of the data implicated by the request.

(ii) A controller may require the consumer to provide additional information only if the request cannot reasonably be verified without the provision of such additional information. A controller must not transfer or process any such additional information provided pursuant to this section for any other purpose and must delete any such additional information without undue delay and in any event within thirty days after the controller has notified the consumer that it has taken action on a request under subdivisions four through seven of this section as described in paragraph (a) of this subdivision.

(iii) If a controller discloses this additional information to any processor or third party for the purpose of verifying a consumer request, it must notify the receiving processor or third party at the time of such disclosure, or as close in time to the disclosure as is reasonably practicable, that such information was provided by the consumer for the sole purpose of verification and cannot be processed for any purpose other than verification.

9. Implementation of rights. Controllers must provide easily accessible and convenient means for consumers to exercise their rights under this article.

10. Non-waiver of rights. Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this article is contrary to public policy and is void and unenforceable.

§ 1203. Controller, processor, and third party responsibilities. 1. Controller responsibilities. (a) Data protection assessments. (i) A controller shall regularly conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes: (A) the processing of personal data for the purposes of targeted advertising, (B) the sale of personal data, (C) the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of (I) unfair or deceptive treatment of, or unlawful disparate impact on consumers, (II) financial, physical or reputational injury to consumers, (III) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns of consumers where such intrusion would be offensive to a reasonable person, or (IV) other substantial injury to consumers; and (D) the processing of sensitive data.

(ii) Data protection assessments conducted pursuant to subparagraph (i) of this paragraph 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 rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The controller shall factor into any such data protection assessment that use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relation-

ship between the controller and the consumer whose personal data will be processed.

(iii) The attorney general may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general, and the controller shall make the data protection assessment available to the attorney general. The attorney general may evaluate the data protection assessment to assess compliance with the provisions of this article. Data protection assessments shall be confidential and shall be exempt from disclosure under the freedom of information law. To the extent any information contained in a data protection assessment disclosure to the attorney general includes information subject to attorney-client privilege or work product protection, such disclosure shall not constitute a waiver of such privilege or protection.

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

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

(vi) Data protection assessment requirements shall apply to processing activities created or generated after the effective date of this article.

(b) Controllers must not engage in unfair, deceptive, or abusive acts or practices with respect to obtaining consumer consent, the processing of personal data, and a consumer's exercise of any rights under this article, including without limitation:

(i) designing a user interface with the purpose or substantial effect of deceiving consumers, obscuring consumers' rights under this article, or subverting or impairing user autonomy, decision-making, or choice; or

(ii) obtaining consent in a manner designed to overpower a consumer's resistance; for example, by making excessive requests for consent.

(c) Controllers must develop, implement, and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal data of consumers including adopting reasonable administrative, technical and physical safeguards appropriate to the volume and nature of the personal data at issue.

(d) (i) A controller shall limit the use and retention of a consumer's personal data to what is (A) necessary to provide the services or goods requested by the consumer, (B) necessary for the internal business operations of the controller and consistent with the disclosures made to the consumer pursuant to section twelve hundred two of this article, or (C) necessary to comply with the legal obligations of the controller.

(ii) At least annually, a controller shall review its retention practices for the purpose of ensuring that it is maintaining the minimum amount of personal data as is necessary for the operation of its business. A controller must securely dispose of all personal data that is no longer (A) necessary to provide the services or goods requested by the consumer, (B) necessary for the internal business operations of the controller and consistent with the disclosures made to the consumer pursuant to section twelve hundred two of this article, or (C) necessary to comply with the legal obligations of the controller.

(e) Non-discrimination. A controller must not discriminate against a consumer for exercising rights under this article, including but not limited to, by:

(i) denying services or goods to consumers;

(ii) charging different prices for services or goods, including through the use of discounts or other benefits; imposing penalties; or providing a different level or quality of services or goods to the consumer; or

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

(f) Agreements with processors. (i) Before making any disclosure, transfer, or sale of personal data to any processor, the controller must enter into a written, signed contract with that processor. Such contract must be binding and clearly set forth 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 must also include requirements that the processor must:

(A) ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

(B) protect the data in a manner consistent with the requirements of this article and at least equal to the security requirements of the controller set forth in their publicly available policies, notices, or similar statements;

(C) process the data only when and to the extent necessary to comply with its legal obligations to the controller unless otherwise explicitly authorized by the controller;

(D) not combine the personal data which the processor receives from or on behalf of the controller with personal data which the processor receives from or on behalf of another person or collects from its own interaction with consumers;

(E) comply with any exercises of a consumer's rights under section twelve hundred two of this article upon the request of the controller, subject to the limitations set forth in section twelve hundred four of this article;

(F) 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 law;

(G) upon the reasonable request of the controller, make available to the controller all data in its possession necessary to demonstrate the processor's compliance with the obligations in this article;

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

(I) a reasonable time in advance before disclosing or transferring the data to any further processors, notify the controller of such a proposed disclosure or transfer and provide the controller an opportunity to approve or reject the proposal; and

(J) engage any further processor pursuant to a written, signed contract that includes the contractual requirements provided in this

paragraph, containing at minimum the same obligations that the processor has entered into with regard to the data.

(ii) A controller must not agree to indemnify, defend, or hold a processor harmless, or agree to a provision that has the effect of indemnifying, defending, or holding the processor harmless, from claims or liability arising from the processor's breach of the contract required by clause (A) of subparagraph (i) of this paragraph or a violation of this article. Any provision of an agreement that violates this subparagraph is contrary to public policy and is void and unenforceable.

(iii) Nothing in this paragraph relieves a controller or a processor from the liabilities imposed on it by virtue of its role in the processing relationship as defined by this article.

(iv) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

(g) Third parties. (i) A controller must not share, disclose, transfer, or sell personal data, or facilitate or enable the processing, disclosure, transfer, or sale to a third party of personal data for which a consumer has exercised their opt-out rights pursuant to subdivision two of section twelve hundred two of this article, or for which consent of the consumer pursuant to subdivision three of section twelve hundred two of this article, has not been obtained or is not currently in effect. Any request for consent to share, disclose, transfer, or sell personal data, or to facilitate or enable the processing, disclosure, transfer, or sale of personal data to a third party of personal data to a third party must clearly include the category of the third party and the processing purposes for which the third party may use the personal data.

(ii) A controller must not share, disclose, transfer, or sell personal data, or facilitate or enable the processing, disclosure, transfer, or sale to a third party of personal data if it can reasonably expect the personal data of a consumer to be used for purposes for which a consumer has exercised their opt-out rights pursuant to subdivision two of section twelve hundred two of this article, or for which the consumer has not consented to pursuant to subdivision three of section twelve hundred two of this article, or if it can reasonably expect that any rights of the consumer provided in this article would be compromised as a result of such transaction.

(iii) Before making any disclosure, transfer, or sale of personal data to any third party, the controller must enter into a written, signed contract. Such contract must be binding and the scope, nature, and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. Such contract must include requirements that the third party:

(A) Process that data only to the extent permitted by the agreement entered into with the controller; and

(B) Provide a mechanism to comply with any exercises of a consumer's rights under section twelve hundred two of this article upon the request of the controller, subject to any limitations thereon as authorized by this article; and

(C) To the extent the disclosure, transfer, or sale of the personal data causes the third party to become a controller, comply with all obligations imposed on controllers under this article.

2. Processor responsibilities. (a) For any personal data that is obtained, received, purchased, or otherwise acquired by a processor, whether directly from a controller or indirectly from another processor, the processor must comply with the requirements set forth in clauses (A) through (J) of subparagraph (i) of paragraph (f) of subdivision one of this section in its role as a processor.

(b) A processor is not required to comply with a request submitted pursuant to this article if (i) the consumer submits the request directly to the processor; and (ii) the processor has processed the consumer's personal data solely in its role as a processor for a controller.

(c) Processors shall be under a continuing obligation to engage in reasonable measures to review their activities for circumstances that may have altered their ability to identify a specific natural person and to update their classifications of data as identified or identifiable accordingly.

(d) A processor shall not engage in any sale of personal data other than on behalf of the controller pursuant to any agreement entered into with the controller.

(e) A processor must adopt appropriate technical and organizational measures to assist a controller in fulfilling the controller's obligation to respond to consumer requests to exercise their rights pursuant to section twelve hundred two of this article, taking into account the nature of the processing and the information available to the processor.

3. Third party responsibilities. For any personal data that is obtained, received, purchased, or otherwise acquired or accessed by a third party from a controller or processor, the third party must:

(a) Process that data only to the extent permitted by any agreements entered into with the controller;

(b) Comply with any exercises of a consumer's rights under section twelve hundred two of this article upon the request of the controller or processor, subject to any limitations thereon as authorized by this article; and

(c) To the extent the third party becomes a controller for personal data, comply with all obligations imposed on controllers under this article.

4. Exceptions. The requirements of this section shall not apply where:

(a) The processing is required by law;

(b) The processing is made pursuant to a request by a federal, state, or local government or government entity; or

(c) The processing significantly advances protection against criminal or tortious activity.

§ 1204. Limitations. 1. This article does not require a controller or processor to do any of the following solely for purposes of complying with this article:

(a) Reidentify deidentified data;

(b) Comply with a verified consumer request to access, correct, or delete personal data pursuant to this article if all of the following are true:

(i) The controller is not reasonably capable of associating the request with the personal data;

(ii) The controller does not associate the personal data with other personal data about the same specific consumer as part of its normal business practice; and

(iii) The controller does not sell the personal data to any third party or otherwise voluntarily disclose or transfer the personal data to any processor or third party, except as otherwise permitted in this article; or

(c) Maintain personal data in identifiable form, or collect, obtain, retain, or access any personal data or technology, in order to be capable of associating a verified consumer request with personal data.

2. The obligations imposed on controllers and processors under this article do not restrict a controller's or processor's ability to do any of the following, to the extent that the use of the consumer's personal data is reasonably necessary and proportionate for these purposes:

(a) Comply with federal, state, or local laws, rules, or regulations, provided that no law enforcement agency or officer thereof shall access personal data without a subpoena or a lawfully executed search warrant, except for the attorney general for the purposes of enforcing this article, except where otherwise provided specifically in federal law;

(b) Investigate, establish, exercise, prepare for, or defend legal claims;

(c) Process personal data necessary to provide the services or goods requested by a consumer; perform a contract to which the consumer is a party; or take steps at the request of the consumer prior to entering into a contract;

(d) Take immediate steps to protect the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;

(e) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action;

(f) Identify and repair technical errors that impair existing or intended functionality; or

(g) Process business contact information, including a natural person's name, position name or title, business telephone number, business address, business electronic mail address, business fax number, or qualifications and any other similar information about the natural person.

3. 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.

4. A controller that receives a request pursuant to subdivisions four through seven of section twelve hundred two of this article, or a processor or third party to whom a controller communicates such a request, may decline to fulfill the relevant part of such request if:

(a) the controller, processor, or third party is unable to verify the request using commercially reasonable efforts, as described in paragraph (c) of subdivision eight of section twelve hundred two of this article;

(b) complying with the request would be demonstrably impossible (for purposes of this paragraph, the receipt of a large number of verified requests, on its own, is not sufficient to render compliance with a request demonstrably impossible);

(c) complying with the request would impair the privacy of another individual or the rights of another to exercise free speech; or

(d) the personal data was created by a natural person other than the consumer making the request and is being processed for the purpose of facilitating interpersonal relationships or public discussion.

§ 1205. Enforcement. 1. (a) Whenever it appears to the attorney general, either upon complaint or otherwise, that any person or persons has engaged in or is about to engage in any of the acts or practices stated to be unlawful under this article, the attorney general may bring an action or special proceeding in the name and on behalf of the people of the state of New York to enjoin any violation of this article, to obtain restitution of any moneys or property obtained directly or indirectly by any such violation, to obtain disgorgement of any profits obtained directly or indirectly by any such violation, to obtain civil penalties of not more than twenty thousand dollars per violation, and to obtain any such other and further relief as the court may deem proper, including preliminary relief.

(b) Any action or special proceeding brought by the attorney general pursuant to this section must be commenced within six years.

(c) Each instance of unlawful processing counts as a separate violation. Unlawful processing of the personal data of more than one consumer counts as a separate violation as to each consumer. Each provision of this article that is violated counts as a separate violation.

(d) In assessing the amount of penalties, the court must consider any one or more of the relevant circumstances presented by any of the parties, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the violator's misconduct, and the violator's financial condition.

2. In connection with any proposed action or special proceeding under this section, the attorney general is authorized to take proof and make a determination of the relevant facts, and to issue subpoenas in accordance with the civil practice law and rules. The attorney general may also require such other data and information as such attorney general may deem relevant and may require written responses to questions under oath. Such power of subpoena and examination shall not abate or terminate by reason of any action or special proceeding brought by the attorney general under this article.

3. Any person, within or outside the state, who the attorney general believes may be in possession, custody, or control of any books, papers, or other things, or may have information, relevant to acts or practices stated to be unlawful in this article is subject to the service of a subpoena issued by the attorney general pursuant to this section. Service may be made in any manner that is authorized for service of a subpoena or a summons by the state in which service is made.

4. (a) Failure to comply with a subpoena issued pursuant to this section without reasonable cause tolls the applicable statutes of limitations in any action or special proceeding brought by the attorney general against the noncompliant person that arises out of the attorney general's investigation.

(b) If a person fails to comply with a subpoena issued pursuant to this section, the attorney general may move in the supreme court to compel compliance. If the court finds that the subpoena was authorized, it shall order compliance and may impose a civil penalty of up to one thousand dollars per day of noncompliance.

(c) Such tolling and civil penalty shall be in addition to any other penalties or remedies provided by law for noncompliance with a subpoena.

5. This section shall apply to all acts declared to be unlawful under this article, whether or not subject to any other law of this state, and shall not supersede, amend or repeal any other law of this state under which the attorney general is authorized to take any action or conduct any inquiry.

§ 1206. Miscellaneous. 1. Preemption: This article preempts the laws, ordinances, regulations, or the equivalent adopted by any local entity regarding the processing, collection, transfer, disclosure, and sale of consumers' personal data by a controller or processor subject to this article.

2. Impact report: The attorney general shall issue a report evaluating this article, its scope, any complaints from consumers or persons, the liability and enforcement provisions of this article including, but not limited to, the effectiveness of its efforts to enforce this article, and any recommendations for changes to such provisions. The attorney general shall submit the report to the governor, the temporary president of the senate, the speaker of the assembly, and the appropriate committees of the legislature within two years of the effective date of this section.

3. Regulatory authority: (a) The attorney general is hereby authorized and empowered to adopt, promulgate, amend and rescind suitable rules and regulations to carry out the provisions of this article, including rules governing the form and content of any disclosures or communications required by this article.

(b) The attorney general may request, and shall receive, data and information from controllers conducting business in New York state, other New York state government entities administering notice and consent regimes, consumer protection and privacy advocates and researchers, internet standards setting bodies, such as the internet engineering taskforce and the institute of electrical and electronics engineers, and other relevant sources, to conduct studies to inform suitable rules and regulations. The attorney general shall receive, upon request, data from other New York state governmental entities.

4. Exercise of rights: Any consumer right set forth in this article may be exercised at any time by the consumer who is the subject of the data or by a parent or guardian authorized by law to take actions of legal consequence on behalf of the consumer who is the subject of the data. An agent authorized by a consumer may exercise the consumer rights set forth in subdivisions four through seven of section twelve hundred two of this article on the consumer's behalf.

§ 4. Severability. If any provision of this act, or any application of any provision of this act, is held to be invalid, that shall not affect the validity or effectiveness of any other provision of this act, or of any other application of any provision of this act, which can be given effect without that provision or application; and to that end, the provisions and applications of this act are severable.

§ 5. This act shall take effect immediately; provided, however, that sections 1201, 1202, 1203, 1204, 1205 and 1206 of the general business law, as added by section three of this act, shall take effect two years after it shall have become a law.