STATE OF NEW YORK

680--B

2021-2022 Regular Sessions

IN ASSEMBLY

(Prefiled)

January 6, 2021

Introduced by M. of A. L. ROSENTHAL, QUART, WEPRIN, D. ROSENTHAL, SIMON, DINOWITZ, PAULIN -- read once and referred to the Committee on Consumer Affairs and Protection -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- recommitted to the Committee on Consumer Affairs and Protection 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 privacy 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

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

LBD00516-05-1

accountable managers of that information. To achieve this, this act 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; the ability to correct inaccurate data and to delete their data; and the ability to challenge certain automated decisions. 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. This act also grants New York consumers who have been injured as the result of a violation a private right of action, which includes reasonable attorneys' fees to a prevailing plaintiff.

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

ARTICLE 42
NEW YORK PRIVACY ACT

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

1. "Automated decision-making" or "automated decision" means a computational process, including one derived from machine learning, artificial intelligence, or any other automated process, involving personal data that results in a decision affecting a consumer.

2. "Biometric information" means any personal data generated from the measurement or specific technological processing of a natural person's biological, physical, or physiological characteristics, including fingerprints, voice prints, iris or retina scans, facial scans or templates, deoxyribonucleic acid (DNA) information, and gait.

3. "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.

4. "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.

5. "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.

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

7. "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.

8. "Data broker" means a person, or unit or units of a legal entity, separately or together, that does business in the state of New York and knowingly collects, and sells to controllers or third parties, the personal data of a consumer with whom it does not have a direct relationship. "Data broker" does not include any of the following:

(a) a consumer reporting agency to the extent that it is covered by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.); or

(b) a financial institution to the extent that it is covered by the Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations.

9. "Deidentified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to a particular consumer, household or device, provided that the processor or controller that possesses 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; and

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

10. "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.

11. "Meaningful human review" means review or oversight by one or more individuals who (a) are trained in the capabilities and limitations of the algorithm at issue and the procedures to interpret and act on the output of the algorithm, and (b) have the authority to alter the automated decision under review.

12. "Natural person" means a natural person 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.

13. "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.

14. "Personal data" means any data that identifies or could reasonably be linked, directly or indirectly, with a specific natural person, household, or device. Personal data does not include deidentified data.

15. "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, location data, or an online or device identifier.

16. "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.

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

18. "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.

19. "Protected health information" has the same meaning as in Title 45 C.F.R., established pursuant to the federal Health Insurance Portability and Accountability Act of 1996.

20. "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" includes enabling, facilitating or providing access to a consumer for targeted advertising. "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; or

(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.

21. "Targeted advertising" means displaying online advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from a consumer's activities over time and across one or more distinctly-branded websites, online applications, or services, to predict the consumer's preferences or interests. It does not include advertising (a) based solely on the context of the consumer's current search query or visit to a website or online application or (b) to a consumer in direct response to the consumer's request for information or feedback.

22. "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.

23. "Verified request" means a request by a consumer or their agent to exercise a right authorized by this article, the authenticity of which has been ascertained by the controller in accordance with paragraph (c) of subdivision eight of section eleven hundred two of this article.

§ 1101. 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 that 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;

(c) controls or processes personal data of five hundred thousand natural persons or more nationwide, and controls or processes personal data of ten thousand consumers or more; or

(d) derives over fifty percent of gross revenue from the sale of personal data, and controls or processes personal data of twenty-five thousand consumers or more.

2. This article does not apply to:

(a) personal data processed by state and local governments, and municipal corporations, for processes other than sale (filing and processing fees are not sale);

(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) information that meets the following criteria:

(i) personal data collected, processed, sold, 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, sold, 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, sold, 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 maintained as employment records, for purposes other than sale;

(vii) protected health information that is lawfully collected by a covered entity or business associate and is governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5);

(viii) patient identifying information for purposes of 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2, as long as such data is not sold in violation of HIPAA or any state or federal law;

(ix) information and documents lawfully created for purposes of the federal Health Care Quality Improvement Act of 1986, and related regulations;

(x) patient safety work product created for purposes of 42 C.F.R. Part 3, established pursuant to 42 U.S.C. Sec. 299b-21 through 299b-26;

(xi) information that is treated in the same manner as information exempt under subparagraph (vii) of this paragraph that is maintained by a covered entity or business associate as defined by HIPAA or a program or a qualified service organization as defined by 42 U.S.C. § 290dd-2,

as long as such data is not sold in violation of HIPAA or any state or federal law;

(xii) deidentified health information that meets all of the following conditions:

(A) it is deidentified in accordance with the requirements for deidentification set forth in Section 164.514 of Part 164 of Title 45 of the Code of Federal Regulations;

(B) it is derived from protected health information, individually identifiable health information, or identifiable private information compliant with the Federal Policy for the Protection of Human Subjects, also known as the Common Rule; and

(C) a covered entity or business associate does not attempt to reidentify the information nor do they actually reidentify the information except as otherwise allowed under state or federal law;

(xiii) patient information maintained by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the covered entity or business associate maintains the patient information in the same manner as protected health information as described in subparagraph (vii) of this paragraph;

(xiv) data collected as part of human subjects research, including a clinical trial, conducted in accordance with the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration; or

(xv) 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;

(d) (i) an activity involving the collection, maintenance, disclosure, sale, 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, sale, 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.

§ 1102. Consumer rights. 1. Right to notice. (a) Notice. Each controller that processes a consumer's personal data must make publicly and

persistently 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 six 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 identity of each third party to whom the controller disclosed, shared, transferred or sold personal data and, for each identified 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) the third party's retention period for each category of personal data processed by the third party or processed on their behalf, or if that is not possible, the criteria used to determine the period, and (D) whether the third party uses the personal data for targeted advertising;

(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; and

(vii) for controllers engaging in targeted advertising, average expected revenue per user (ARPU) or a similar metric for the most recent fiscal year for the region that covers New York.

(b) Notice requirements.

(i) The notice must be written in easy-to-understand language at an eighth grade reading level or below.

(ii) The categories of personal data processed and purposes for which each category of personal data is processed must be described 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 reasonable 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. Opt-in consent. (a) A controller must obtain freely given, specific, informed, and unambiguous opt-in consent from a consumer to:

(i) process the consumer's personal data for any purpose other than those in subdivision two of section eleven hundred five 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 personal data that may be less protective of the consumer's personal 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 must be provided to the consumer, prior to processing their personal data, in a standalone disclosure that is sepa-

rate and apart from any contract or privacy policy. The request for consent must:

(i) 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 personal data to third parties, identify each such third party, 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 for each third party state if such sharing, disclosure, transfer, or sale enables or involves targeted advertising. The details of identities 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 personal 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) To the extent that a controller must process internet protocol addresses, system configuration information, URLs of referring pages, locale and language preferences, keystrokes, or any other data that individually or collectively may comprise personal data in order to obtain a consumer's freely given, specific, informed, and unambiguous opt-in consent, the controller must:

(i) process only the personal data necessary to request freely given, specific, informed, and unambiguous opt-in consent;

(ii) process the personal data solely to request freely given, specific, informed, and unambiguous opt-in consent; and

(iii) promptly delete the personal data if consent is withheld, denied, or withdrawn.

(h) Controllers must not request consent from a consumer who has previously withheld or denied consent, unless consent is necessary to provide the services or goods requested by the consumer.

(i) 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 not to be subject to targeted advertising or the sale of their personal data as a denial of consent under this act. 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.

(j) A controller must not discriminate against a consumer for 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.

(k) A controller may, with the consumer's freely given, specific, informed, and unambiguous opt-in consent given pursuant to this section, operate a program in which information, products, or services sold to the consumer are discounted based solely on such consumer's prior purchases from the controller, provided that the personal data used to operate such program is processed solely for the purpose of operating such program.

(l) 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 prior to such transaction shall be deemed withdrawn.

3. Right to access. Upon the verified 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 identity of each processor or third party to whom the controller disclosed, transferred, or sold the consumer's personal data and, for each identified 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.

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

5. Right to correct. (a) Upon the verified 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 processor or 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 processors or third parties to do the same for any further processors or 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.

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

(i) within forty-five days after receiving the verified request, delete any or all 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 processor or 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 processors or third parties to do the same for any further processors or 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.

(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 processor or 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.

7. Automated decision-making. (a) Whenever a controller makes an automated decision involving solely automated processing that materially contributes to a denial of financial or lending services, housing, public accommodation, insurance, health care services, or access to basic necessities, such as food and water, the controller must:

(i) disclose in a clear, conspicuous, and consumer-friendly manner that the decision was made by a solely automated process;

(ii) provide an avenue for the affected consumer to appeal the decision, which must at minimum allow the affected consumer to (A) formally contest the decision, (B) provide information to support their position, and (C) obtain meaningful human review of the decision; and

(iii) explain the process to appeal the decision.

(b) A controller must respond to a consumer's appeal within forty-five days of receipt of the appeal. That period may be extended once by forty-five additional days where reasonably necessary, taking into account the complexity and number of appeals. The controller must inform the consumer of any such extension within forty-five days of receipt of the appeal, together with the reasons for the delay.

(c) (i) A controller or processor engaged in automated decision-making affecting financial or lending services, housing, public accommodation, insurance, education enrollment, employment, health care services, or access to basic necessities, such as food and water, or engaged in assisting others in automated decision-making in those fields, must annually conduct an impact assessment of such automated decision-making that:

(A) describes and evaluates the objectives and development of the automated decision-making processes including the design and training data used to develop the automated decision-making process, how the automated decision-making process was tested for accuracy, fairness, bias and discrimination; and

(B) assesses whether the automated decision-making system produces discriminatory results on the basis of a consumer's or class of consumers' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability.

(ii) A controller or processor must utilize an external, independent auditor or researcher to conduct such assessments.

(iii) A controller or processor must make publicly available in a manner accessible online all impact assessments prepared pursuant to this section, retain all such impact assessments for at least six years, and make any such retained impact assessments available to any state, federal, or local government authority upon request.

(iv) For purposes of this paragraph, the limitations to jurisdictional scope set forth in paragraphs (b) and (c) of subdivision two of section eleven hundred one of this article shall not apply.

8. Responding to requests. (a) A controller must take action under subdivisions three through six of this section and inform the consumer of any actions taken without undue delay and in any event within forty-five days of receipt of the request. That period may be extended once by forty-five 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 forty-five 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.

(b) A controller shall permit the exercise of rights and carry out its obligations set forth in subdivisions three through six 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 forty-five days after the controller has notified the consumer that it has taken action on a request under subdivisions two through five 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.

§ 1103. Controller, processor, and third party responsibilities. 1. Controller responsibilities. (a) Data protection assessment. A controller shall regularly conduct and document a data protection assessment for processing activities that present a heightened risk of harm to the consumer. Such assessment must 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, or class of consumers, associated with the processing, as mitigated by safeguards that the controller can employ to reduce the risks. The controller shall factor into this assessment the use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, with the goal of restricting or prohibiting such processing if the risks of harm to the consumer outweigh the benefits resulting from the processing to the consumer. Processing that presents a heightened risk of harm to the consumer includes the following:

(i) processing that may benefit the controller to the detriment of the consumer;

(ii) processing that would be unexpected and highly offensive to a reasonable consumer;

(iii) processing personal data for purposes of targeted advertising;

(iv) sale of personal data; and

(v) processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of:

(A) unfair or deceptive treatment, or unlawful disparate impact on, consumers or a class of consumers;

(B) financial, physical, psychological or reputational injury to consumers, or a class of consumers;

(C) a physical or otherwise 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

(D) other substantial injury to consumers.

(b) Duty of loyalty. (i) A controller must notify the consumer, or class of consumers, of the interest that may be harmed in advance of requesting consent and as close in time to the processing as practicable where it is reasonably foreseeable to the controller that a process presents a heightened risk of harm to the consumer or class of consumers.

(ii) 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:

(A) 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 in order to obtain consent; or

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

(c) Duty of care. (i) (A) Controllers must, on at least an annual basis, conduct and document risk assessments of all current processing of personal data.

(B) Risk assessments must assess at a minimum:

(I) the nature, sensitivity and context of the personal data that the controller processes;

(II) the nature, purpose, and value of the processes;

(III) any risks or harms to consumers actually or potentially arising out of the processes, including physical, financial, psychological, or reputational harms;

(IV) the adequacy and effect of safeguards implemented by the controllers;

(V) the sufficiency of the controller's notices to consumers at describing and obtaining consent concerning the processes; and

(VI) the adequacy of the safeguards and monitoring practices of processors and third parties to whom the controller has provided personal data.

(C) The controller must retain risk assessments for at least six years and make risk assessments available to the attorney general upon request.

(ii) 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.

(iii) (A) A controller shall limit the use and retention of a consumer's personal data to what is necessary to provide a service or good requested by a consumer or for purposes for which the consumer has provided freely given, specific, informed, and unambiguous opt-in consent.

(B) 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 dispose of all personal data that is no longer (I) necessary to provide the services or goods requested by the consumer, (II) necessary for the internal business operations of the controller and consistent with the disclosures made to the consumer pursuant to section eleven hundred two of this article, or (III) necessary to comply with the legal obligations of the controller.

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

(A) denying services or goods to consumers;

(B) 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

(C) 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.

(ii) This paragraph does not apply to a controller's conduct with respect to opt-in consent, in which case paragraph (j) of subdivision two of section eleven hundred two of this article governs.

(e) 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 act 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 eleven hundred two of this article upon the request of the controller, subject to the limitations set forth in section eleven hundred five 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 act;

(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 act. 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.

(f) Third parties. (i) A controller must not share, disclose, transfer, or sell personal data, or facilitate or enable the processing, disclosure, transfer, or sale of personal data to a third party for which consent of the consumer pursuant to subdivision two of section eleven 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 must clearly include the identity 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 of personal data if it can reasonably expect the personal data of a consumer to be used for purposes that the consumer has not consented to pursuant to subdivision two of section eleven 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 eleven 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 (e) of subdivision one of this section.

(b) A processor is not required to comply with a request by the consumer submitted pursuant to this article by a consumer directly to the processor to the extent that 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.

3. Third party responsibilities. (a) 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:

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

(ii) Process only the personal data necessary for purposes for which freely given, specific, informed, and unambiguous opt-in consent is in effect, as conveyed by the controller, limit the use and retention of that data to what is necessary for such purposes, and shall immediately delete such personal data when notified that the consent is withheld, denied, or withdrawn;

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

(iv) 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.

§ 1104. Data brokers. 1. A data broker, as defined under this article, must:

(a) Annually, on or before January thirty-first following a year in which a person meets the definition of data broker in this article:

(i) Register with the attorney general;

(ii) Pay a registration fee of one hundred dollars or as otherwise determined by the attorney general pursuant to the regulatory authority granted to the attorney general under this article, not to exceed the reasonable cost of establishing and maintaining the database and informational website described in this section; and

(iii) Provide the following information:

(A) the name and primary physical, email, and internet website address of the data broker;

(B) the name and business address of an officer or registered agent of the data broker authorized to accept legal process on behalf of the data broker;

(C) a statement describing the method for exercising consumers rights under section eleven hundred two of this article;

(D) a statement whether the data broker implements a purchaser credentialing process; and

(E) any additional information or explanation the data broker chooses to provide concerning its data collection practices.

2. Notwithstanding any other provision of this article, any controller that conducts business in the state of New York must:

(a) annually, on or before January thirty-first following a year in which a person meets the definition of controller in this act, provide

to the attorney general a list of all data brokers or persons reasonably believed to be data brokers to which the controller provided personal data in the preceding year; and

(b) not sell a consumer's personal data to a data broker that is not registered with the attorney general.

3. The attorney general shall establish, manage and maintain a statewide registry on its internet website, which shall list all registered data brokers and make accessible to the public all the information provided by data brokers pursuant to this section. Printed hard copies of such registry shall be made available upon request and payment of a fee to be determined by the attorney general.

4. A data broker that fails to register as required by this section or submits false information in its registration is, in addition to any other injunction, penalty, or liability that may be imposed under this article, liable for civil penalties, fees, and costs in an action brought by the attorney general as follows: (a) a civil penalty of one thousand dollars for each day the data broker fails to register as required by this section or fails to correct false information, (b) an amount equal to the fees that were due during the period it failed to register, and (c) expenses incurred by the attorney general in the investigation and prosecution of the action as the court deems appropriate.

§ 1105. 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;

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

(c) Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;

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

(e) 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;

(f) 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;

(g) 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;

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

(i) 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 three through six of section eleven 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 eleven 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.

§ 1106. Enforcement and private right of action. 1. 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 fifteen thousand dollars per violation, and to obtain any such other and further relief as the court may deem proper, including preliminary relief.

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

(b) 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.

(c) 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 he or she 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 five hundred 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.

6. Any consumer who has been injured by a violation of subdivision two, seven or eight of section eleven hundred two of this article may bring an action in his or her own name to enjoin such unlawful act or practice and to recover his or her actual damages or one thousand dollars, whichever is greater. The court may also award reasonable attorneys' fees to a prevailing plaintiff. Actions pursuant to this section may be brought on a class-wide basis.

§ 1107. Miscellaneous. 1. Preemption: This article does not annul, alter, or affect 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, except to the extent those laws, ordinances, regulations, or the equivalent create requirements or obli-

gations that conflict with or reduce the protections afforded to consumers under 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 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 three through six of section eleven hundred two of this act on the consumers behalf.

§ 4. This act shall take effect immediately; provided, however, that sections 1101, 1102, 1103, 1105, 1106 and 1107 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 but the private right of action authorized by subdivision 6 of section 1106 of the general business law shall take effect three years after such section shall have become a law.