STATE OF NEW YORK

9642--A

IN ASSEMBLY

January 21, 2026

Introduced by M. of A. TORRES, SIMON -- 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

AN ACT to amend the general business law, in relation to requiring the registration of data brokers and establishing a data deletion mechanism for consumers

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

Section 1. The general business law is amended by adding a new article 42-A to read as follows:

ARTICLE 42-A
DATA BROKERS

Section 1150. Definitions.
1151. Registration of data brokers.
1152. Data deletion mechanism.
1153. Audit.
1154. Data broker website disclosure requirements.
1155. Data brokers; comprehensive information security program.
1156. Rulemaking.
1157. Enforcement.
1158. Exemptions.

§ 1150. Definitions. The following definitions apply throughout this article unless the context clearly requires otherwise:

1. "Artificial intelligence system or model" means an artificial intelligence that can generate derived synthetic content, including text, images, video, and audio, that emulates the structure and characteristics of the system's training data.

2. "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. The term "aggregate consumer information" shall not include one or more individual consumer records that have been deidentified.

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

LBD14455-05-6

3. "Biometric data" means an individual's physiological, biological, or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that can be used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity. The term "biometric information" includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information. "Biometric data" 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.

4. "Business" means:

(a) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the state of New York, and that satisfies one or more of the following thresholds:

(i) as of January first of the relevant calendar year, had annual gross revenues in excess of ten million dollars in the preceding calendar year;

(ii) alone or in combination, annually buys, sells, or shares the personal information of one hundred thousand or more consumers or households; or

(iii) derives fifty percent or more of its annual revenues from selling or sharing consumers' personal information;

(b) (i) Any entity that controls or is controlled by a business, as defined in paragraph (a) of this subdivision, and that shares common branding with such business and with whom such business shares consumers' personal information.

(ii) For the purposes of this paragraph, the following terms shall have the following meanings:

(1) "Control" or "controlled" means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of an entity, whether through the ownership of voting securities, by contract, or otherwise;

(2) "Common branding" means a shared name, service mark, or trademark that the average consumer would understand that two or more entities are commonly owned;

(c) A joint venture or partnership composed of businesses in which each business has at least a forty percent interest. For purposes of this article, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business; or

(d) A person that does business in New York, that is not covered by paragraph (a), (b), or (c) of this subdivision, and that voluntarily certifies to the attorney general that it is in compliance with, and agrees to be bound by, this article.

5. "Collects", "collected", or "collection" means buying, renting, gathering, obtaining, receiving, sharing or accessing any personal information pertaining to a consumer by any means, including but not limited to, receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.

6. "Consent" means any freely given, specific, informed, and unambiguous indication of a consumer's wishes by which such consumer, or such consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for such consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to such consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, shall not constitute consent. Hovering over, muting, pausing, or closing a given piece of content shall not constitute consent. Agreement obtained through use of dark patterns shall not constitute consent.

7. "Consumer" means a natural person who is an individual who is in New York state for other than a transitory purpose, and every individual who is domiciled in New York state who is outside the state.

8. "Contractor" means a person to whom a business makes available a consumer's personal information for a business purpose, pursuant to a written contract with such business, provided that such contract:

(a) prohibits the contractor from:

(i) selling or sharing such personal information;

(ii) retaining, using, or disclosing such personal information for any purpose other than for the business purposes specified in such contract, including retaining, using, or disclosing such personal information for a commercial purpose other than the business purposes specified in such contract, or as otherwise permitted by this article;

(iii) retaining, using, or disclosing such personal information outside of the direct business relationship between the contractor and such business; and

(iv) combining such personal information that the contractor receives pursuant to a written contract with such business with personal information that it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer;

(b) includes a certification made by the contractor that the contractor understands the restrictions provided for in accordance with paragraph (a) of this subdivision and will comply with them;

(c) permits the business to monitor the contractor's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every twelve months; and

(d) provides that if the contractor engages any other person to assist it in processing personal information for a business purpose on behalf of such business, or if any other person engaged by such contractor engages another person to assist in processing personal information for such business purpose, it shall notify such business of such engagement, and such engagement shall be pursuant to a written contract binding such other person to comply with all the requirements set forth in this subdivision.

9. "Cross-context behavioral advertising" means the targeting of advertising and marketing to a consumer based on such consumer's personal information obtained from such consumer's activity across busi-

nesses, distinctly branded internet websites, applications, or services with which such consumer intentionally interacts.

10. "Dark patterns" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation issued by the attorney general.

11. (a) "Data broker" means a business that knowingly collects and sells to third parties the personal information of a consumer with whom such business either:

(i) does not have a direct relationship; and/or

(ii) collects, retains or sells personal information outside of the consumer-facing business with which the consumer intends and expects to interact through informed consent.

(b) The term "data broker" shall not include any of the following:

(i) a federal, state, tribal, territorial, or local governmental entity, including a body, authority, board, bureau, commission, district, agency, or political subdivision of a governmental entity; or

(ii) an entity that serves as a congressionally designated nonprofit, national resource center, or clearinghouse to provide assistance to victims, families, child-serving professionals, and the general public on missing and exploited children issues.

(c) For the purposes of this subdivision, "direct relationship" shall mean a consumer has intentionally and unambiguously interacted with a business for the purpose of accessing, purchasing, using, requesting, or obtaining information about the business's products or services. A business shall not be deemed to have a direct relationship with a consumer merely because the business collects personal information of the consumer.

12. "Deidentified" means information that cannot be used to infer information about, or otherwise be linked to, a particular consumer, provided that businesses that possess such information shall:

(a) take necessary measures to ensure that such information cannot be associated with a consumer or household;

(b) publicly, and within any contract in which such business acquired such information, commit to maintaining and using such information only in deidentified form;

(c) not attempt to reidentify such information, except that such business may attempt to reidentify such information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision; and

(d) contractually (i) prohibit any recipients of such information from reidentifying such information, and (ii) require compliance with all provisions of this subdivision.

13. "Designated methods for submitting deletion requests" means a mailing address, email address, internet web page, internet web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this article, and any new, consumer-friendly means of contacting a business, as approved in writing by the attorney general.

14. "Developer of an artificial intelligence system or model" means a person, partnership, corporation, firm, organization or other entity that designs, codes, produces, trains or substantially modifies an artificial intelligence system.

15. "Device" means any physical object that is capable of connecting to the internet, directly or indirectly, or to another device.

16. "Foreign actor" means either:

(a) the government of a foreign adversary country; or

(b) a partnership, association, corporation, organization, or other combination of persons organized under the laws of or having its principal place of business in a foreign adversary country.

17. "Foreign adversary country" has the same meaning as "covered nation" as defined in Section 4872 of Title 10 of the United States Code.

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

19. "Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

20. "Intentionally interacts" means when a consumer intends to interact with a person, or disclose personal information to a person, via one or more deliberate interactions, including visiting such person's internet website or purchasing a good or service from such person. Hovering over, muting, pausing, or closing a given piece of content shall not constitute a consumer's intent to interact with a person.

21. "Minor" means a natural person under the age of eighteen.

22. "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization, entity or group of persons acting in concert.

23. (a) "Personal information" means information, however maintained, that identifies, relates to, describes, is capable of being associated with, or could be linked, directly or indirectly, with a particular consumer or household, including, but not limited to, the following:

(i) identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;

(ii) any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, such individual's name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information;

(iii) characteristics of protected classifications under New York or federal law;

(iv) commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;

(v) biometric information;

(vi) internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement;

(vii) geolocation data;

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

(ix) professional or employment-related information;

(x) education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99);

(xi) inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting such consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes; and

(xii) sensitive personal information;

(b) The term "personal information" shall not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. For purposes of this paragraph, "publicly available" means any of the following:

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

(ii) information that a business has a reasonable basis to believe is lawfully and intentionally made available to the general public by the consumer or from widely distributed media; or

(iii) information made available by a person to whom the consumer has intentionally disclosed such information if such consumer has consented to such information not being restricted to a specific audience.

(c) The term "publicly available" shall not mean biometric information collected by a business about a consumer.

(d) The term "personal information" shall not include:

(i) consumer information that is deidentified and aggregate consumer information; and

(ii) information that would not otherwise be made public but for a data breach.

(e) The term "personal information" may exist in various formats, including, but not limited to, all of the following:

(i) physical formats, including paper documents, printed images, vinyl records, or video tapes;

(ii) digital formats, including text, image, audio, or video files; or

(iii) abstract digital formats, including compressed or encrypted files, metadata, or artificial intelligence systems that are capable of outputting personal information.

24. "Precise geolocation data" means any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of eighteen hundred fifty feet, except as prescribed by regulations.

25. "Probabilistic identifier" means the identification of a consumer or such consumer's device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information under subdivision twenty-three of this section.

26. "Processing" means any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means.

27. "Processor" shall mean a person who collects, processes, or transfers personal information on behalf of, and at the direction of, a data broker or another processor, or a Federal, state, tribal, or local government entity.

28. "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.

29. "Pseudonymize" or "pseudonymization" means the processing of personal information in a manner that renders such personal information no longer attributable to a specific consumer without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that such personal information is not attributed to an identified or identifiable consumer and shall not be reidentified through methods such as inference, hashing manipulation, or any other computational or analytical technique.

30. "Reproductive health care data" means any of the following:

(a) information about a consumer searching for, accessing, procuring, using, or otherwise interacting with goods or services associated with the human reproductive system, which includes goods such as contraception including but not limited to condoms or birth-control pills, prenatal and fertility vitamins and supplements, menstrual-tracking apps, and hormone-replacement therapy, and shall further include, but not be limited to, services such as sperm- and egg-freezing, In Vitro Fertilization, abortion care, vasectomies, sexual health counseling; treatment or counseling for sexually transmitted infections, erectile dysfunction, and reproductive tract infections; and precise geolocation information about such treatments; or (b) information about a consumer's sexual history and family planning, which includes information such consumer inputs into a dating app about their history of sexually transmitted infections or desire to have children.

31. "Security and integrity" means the ability of:

(a) networks or information systems to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information;

(b) businesses to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions and to help prosecute those responsible for those actions; or

(c) businesses to ensure the physical safety of natural persons.

32. (a) "Sell", "selling", "sale", or "sold" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by a business to a third party for monetary or other valuable consideration.

(b) For purposes of this article, a business shall not be deemed to sell personal information when:

(i) a consumer uses or directs such business to intentionally:

(1) disclose personal information; or

(2) interact with one or more third parties;

(ii) such business uses or shares an identifier for a consumer who has opted out of the sale of such consumer's personal information or limited the use of such consumer's sensitive personal information solely for the purposes of alerting persons to or for whom such consumer has opted out of the sale of such consumer's personal information or limited the use of such consumer's sensitive personal information; provided such identifier does not disclose any personal information other than what is necessary for such alert; or

(iii) such business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which such third party assumes control of all or part of such business, provided that as a condition to such transaction, the third party contractually agrees to assume all responsibilities of the transferring business with respect to such

personal information, and comply with this article in all respects. A third party shall not use or share the personal information of a consumer in a manner that is inconsistent with the promises made at the time of collection. This subparagraph shall not authorize a business to make retroactive privacy policy changes or make other changes in their privacy policy.

33. "Sensitive personal information" means:

(a) personal information that reveals:

(i) a consumer's social security, driver's license, state identification card, or passport number;

(ii) a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;

(iii) a consumer's precise geolocation;

(iv) a consumer's racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership;

(v) the contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication;

(vi) a consumer's sexuality or gender identity;

(vii) reproductive health care data;

(viii) a consumer's genetic data; or

(ix) a consumer's neural data, meaning information that is generated by measuring the activity of such consumer's central or peripheral nervous system, and that is not inferred from nonneural information; or

(b) the processing of biometric information for the purpose of uniquely identifying a consumer, including but not limited to:

(i) personal information collected and analyzed concerning a consumer's health; or

(ii) personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

34. "Service" or "services" means work, labor, and services, including services furnished in connection with the sale or repair of goods.

35. (a) "Service provider" means a person that processes personal information on behalf of a business and that receives from or on behalf of such business a consumer's personal information for a business purpose pursuant to a written contract, provided that such contract prohibits such person from:

(i) selling or sharing such personal information;

(ii) retaining, using, or disclosing such personal information for any purpose other than for the business purposes specified in the contract for such business, including retaining, using, or disclosing such personal information for a commercial or business purpose other than the business purposes specified in the contract with such business, or as otherwise permitted by this article;

(iii) retaining, using, or disclosing the information outside of the direct business relationship between the service provider and such business; or

(iv) combining such personal information that the service provider receives from, or on behalf of, such business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer. Such contract shall permit the business to monitor such service provider's compliance with such contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every twelve months.

(b) If a service provider engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by such service provider engages another person to assist in processing personal information for such business purpose, it shall notify such business of such engagement, and such engagement shall be pursuant to a written contract binding such other person to comply with all the requirements set forth in paragraph (a) of this subdivision.

(c) Any information acquired by a service provider for the purpose of providing verification, authentication or similar service 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.

36. (a) "Share", "shared", or "sharing" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by a business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

(b) For purposes of this article, a business shall not be deemed to share personal information when:

(i) a consumer uses or directs such business to intentionally disclose personal information or intentionally interact with one or more third parties;

(ii) a consumer directs such business to intentionally interact with one or more third parties and such consumer has provided consent for the business to disclose personal information to such third party or parties;

(iii) such business uses or shares an identifier for a consumer who has opted out of the sharing of such consumer's personal information or limited the use of such consumer's sensitive personal information, solely for the purposes of alerting persons to or for whom such consumer has opted out of the sharing of such consumer's personal information or limited the use of such consumer's sensitive personal information, provided such identifier does not disclose any personal information other than what is necessary for such alert; or

(iv) such business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which such third party assumes control of all or part of such business, provided that as a condition to such transaction, the third party contractually agrees to assume all responsibilities of the transferring business with respect to such personal information, and comply with this article in all respects. A third party shall not use or share the personal information of a consumer in a manner that is inconsistent with the promises made at the time of collection. This subparagraph shall not authorize a business to make retroactive privacy policy changes or make other changes in their privacy policy.

37. "Third party" means a person who is not any of the following:

(a) the business with whom a consumer intentionally interacts and that collects personal information from such consumer as part of such consumer's current interaction with such business under this article;

(b) a service provider to the business;

(c) a contractor to the business; or

(d) a processor to the business.

38. "Unique identifier" or "unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a household, a family, or a device that is linked to a consumer, household, or family, over time and across different services, including, but not limited to: a device identifier; an internet protocol address; device fingerprinting; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device that is linked to a consumer, household or family. For purposes of this subdivision, the term "family" means a custodial parent or guardian and any children under eighteen years of age over which the parent or guardian has custody.

39. "Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of such consumer's minor child, or by a person who has power of attorney or is acting as a conservator for such consumer, and that the business can verify, using commercially reasonable methods, pursuant to any regulations adopted by the attorney general to be such consumer about whom the business has collected personal information.

40. "Authorized agent" means:

(a) a person designated by a consumer to act on the consumer's behalf;

(b) a parent or legal guardian that acts on behalf of the parent's child or on behalf of a child for whom the guardian has legal responsibility; or

(c) a guardian or conservator that acts on behalf of a consumer that is subject to a guardianship, conservatorship, or other protective arrangement.

§ 1151. Registration of data brokers. 1. Each data broker shall:

(a) No later than sixty days after meeting the definition of data broker in this article:

(i) Register with the attorney general pursuant to this section;

(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 to the attorney general in a form and manner determined by the attorney general:

(A) all names used by the data broker, and its primary physical, email, and internet website address.

(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) the number of requests received and the number of such requests complied with, complied with in part, or denied under section eleven hundred fifty-two of this article.

(D) the median and the mean number of days within which the data broker responded to requests under section eleven hundred fifty-two of this article.

(E) whether the data broker collected personal information of minors.

(F) whether the data broker collects or infers consumers' names, dates of birth, ZIP codes, email addresses, or phone numbers.

(G) whether the data broker collects or infers consumers' account login or account number in combination with any required security code,

access code, or password that would permit access to a consumer's account with a third party.

(H) whether the data broker collects or infers consumers' drivers' license numbers, New York identification card numbers, tax identification numbers, social security numbers, passport numbers, military identification numbers, or other unique identification numbers issued on a government document commonly used to verify the identity of a specific individual.

(I) whether the data broker collects or infers consumers' mobile advertising identification numbers, connected television identification numbers, or vehicle identification numbers (VIN).

(J) whether the data broker collects or infers consumers' citizenship data, including immigration status.

(K) whether the data broker collects or infers consumers' union membership status.

(L) whether the data broker collects or infers consumers' sexual orientation status.

(M) whether the data broker collects or infers consumers' gender identity and gender expression data.

(N) whether the data broker collects or infers consumers' biometric data.

(O) whether the data broker collects or infers consumers' precise geolocation.

(P) whether the data broker collects or infers consumers' reproductive health care data.

(Q) whether the data broker collects or infers consumers' protected health information.

(R) whether the data broker has shared or sold consumers' data to a foreign actor in the past five years.

(S) whether the data broker has shared or sold consumers' data to the federal government in the past five years.

(T) whether the data broker has shared or sold consumers' data to other state governments in the past five years.

(U) whether the data broker has shared or sold consumers' data to law enforcement in the past five years, unless that data was shared pursuant to a subpoena or court order.

(V) whether the data broker has shared or sold consumers' data to a developer of an artificial intelligence system or model in the past five years.

(W) up to three, but no fewer than one, of the most common types of personal information that the data broker collects.

(X) beginning January first, two thousand thirty, whether the data broker has undergone an audit under this article, and, if so, the most recent year that the data broker has submitted a report resulting from the audit and any related materials to the attorney general.

(Y) a link to a page on the data broker's internet website that:

(I) details how consumers may exercise their privacy rights by doing all of the following:

a. Deleting personal information.

b. Correcting inaccurate personal information.

c. Learning what personal information is being collected and how to access that personal information.

d. Learning what personal information is being sold or shared and to whom.

e. Learning how to opt out of the sale or sharing of personal information.

f. Learning how to limit the use and disclosure of sensitive personal information.

(II) does not make use of any dark patterns.

(Z) whether and to what extent the data broker or any of its subsidiaries is regulated by any of the following:

(I) the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.);

(II) the Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations;

(III) 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 federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191); or

(IV) any other law, rule, or regulation governing data brokers or any of its subsidiaries.

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

(b) be subject to any rules and regulations promulgated under this article.

2. The attorney general shall create a webpage on the state website which includes all information regarding all data brokers registered within the state and the deletion mechanism created under section eleven hundred fifty-two of this article.

§ 1152. Data deletion mechanism. 1. The attorney general shall establish a data deletion mechanism within one year of the effective date of this section. Such data deletion mechanism shall:

(a) implement and maintain reasonable security procedures and practices, including, but not limited to, administrative, physical, and technical safeguards appropriate to the nature of the information and the purposes for which the personal information will be used and to protect consumers' personal information from unauthorized use, disclosure, access, destruction, or modification.

(b) allow a consumer, through a single verifiable consumer request, to request that every data broker that maintains any personal information delete any personal information related to that consumer held by the data broker or associated service provider, contractor, or subsidiary.

(c) allow a consumer to selectively exclude specific data brokers from a request made under paragraph (b) of this subdivision.

(d) allow a consumer to make a request to alter a previous request made under this section after at least forty-five days have passed since the consumer last made a request under this section.

(e) allow a consumer to request the deletion of all personal information related to that consumer through a single deletion request.

(f) permit a consumer to securely submit information in one or more privacy-protecting ways determined by the attorney general to aid in the deletion request.

(g) allow data brokers registered with the attorney general to determine whether an individual has submitted a verifiable consumer request to delete the personal information related to that consumer and shall not allow the disclosure of any additional personal information when the data broker accesses the accessible deletion mechanism unless otherwise specified in this article.

(h) allow a consumer to make a request under this section using an internet service operated by the attorney general.

(i) not charge a consumer to make a request under this section.

(j) allow a consumer to make a request under this section in any of the twelve most commonly spoken languages in New York state, consistent with section two hundred two-a of the executive law, for whom personal information has been collected by data brokers.

(k) comply with section one hundred three-d of the state technology law.

(l) be readily accessible and usable by consumers with disabilities.

(m) support the ability of a consumer's authorized agents to aid in the deletion request.

(n) allow the consumer, or their authorized agent, to verify the status of the consumer's deletion request.

(o) provide a description of:

(i) the deletion permitted by this section including the actions required of data brokers described in this section;

(ii) the process for submitting a deletion request pursuant to this section; and

(iii) examples of the types of information that may be deleted.

2. Beginning six months after the establishment of the data deletion mechanism, the attorney general shall make each request submitted pursuant to this section available to each applicable data broker without undue delay and each data broker shall access the accessible deletion mechanism established pursuant to subdivision one of this section at least once every forty-five days.

3. Beginning six months after the establishment of the data deletion mechanism, each data broker shall:

(a) at least once every forty-five days, process all deletion requests made pursuant to this section and delete all personal information related to the consumers making verifiable consumer requests consistent with the requirements of this section within forty-five days of receiving such requests and direct all service providers, contractors, and subsidiaries associated with the data broker to delete all personal information in their possession related to the consumers making such verifiable consumer requests;

(b) cease all processing activities of personal information related to the consumers making the verifiable consumer requests promptly and without reasonable delay not to exceed five days after receiving a verifiable consumer request; and

(c) where a data broker denies a consumer request to delete under this section because the request cannot be verified, process the request as an opt-out of the sale or sharing of the consumer's personal information within forty-five days of receiving such request and direct all service providers, contractors, and subsidiaries associated with the data broker to process the request as an opt-out of the sale or sharing of the consumer's personal information, regardless of whether such data broker has an existing policy providing for consumers to opt out.

4. (a) Notwithstanding any other provision of this section, a data broker shall not be required to delete a consumer's personal information to the extent such personal information is:

(i) used by a consumer reporting agency to furnish a consumer report pursuant to the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.);

(ii) strictly necessary to fulfill a specific legal requirement on behalf of a business to which the data broker is bound by a written contract to fulfill that legal requirement;

(iii) used to prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, or to preserve the phys-

ical security and technical integrity of systems or investigate, report, or prosecute those responsible for any such action;

(iv) strictly necessary to investigate, establish, exercise, prepare for, or defend a legal claim; or

(v) used to comply with a civil, criminal or regulatory inquiry, investigation, subpoena, or summons by federal, state, municipal, or other governmental authority, provided that a business that has received direction from a law enforcement agency not to delete the personal information of a consumer who has requested deletion of such consumer's personal information shall not use such consumer's personal information for any purpose other than retaining it to produce to law enforcement in response to a court-issued subpoena, order, or warrant unless such consumer's deletion request is subject to an exemption from deletion under this article.

(b) Personal information not required to be deleted under paragraph (a) of this subdivision shall be separated or segregated from data used for any other purpose, deleted immediately upon the expiration of the legal or contractual requirement, and only be used for purposes directly related to such exceptions and shall not be used or disclosed for any other purpose.

5. Where a consumer has submitted a deletion request and a data broker has deleted the consumer's data pursuant to this section, the data broker shall:

(a) delete all personal information of the consumer at least once every forty-five days pursuant to this section unless the consumer requests otherwise or the deletion is not required pursuant to subdivision four of this section; and

(b) not sell or share new personal information of the consumer unless the consumer requests otherwise unless such selling or sharing is permitted under subdivision four of this section, provided that, where selling, sharing or retention of personal information is permitted, such consumer shall receive notice of continued retention of personal information.

6. The attorney general may charge an access fee to a data broker when the data broker accesses the data deletion mechanism that does not exceed the reasonable costs of providing that access.

7. A request made pursuant to this section shall be deemed received on the date such request is made available to the data broker through the accessible deletion mechanism established pursuant to this section.

§ 1153. Audit. Three years after the effective date of this section and every three years thereafter, each data broker shall undergo an audit by an independent third party to determine compliance with this article. Each data broker shall submit a report resulting from the audit written by such independent third party in a form determined by the attorney general and any other materials required by the attorney general to the attorney general within five business days of a written request by the attorney general. Data brokers shall maintain such reports and any required materials for at least six years.

§ 1154. Data broker website disclosure requirements. 1. On or before July first following each calendar year, or by such other date as the attorney general may establish by regulation in which a business meets the definition of a data broker as provided in this article, the business shall clearly and conspicuously post their privacy policy on their website as well as do all of the following:

(a) Disclose the number of consumer deletion requests made to the data broker pursuant to section eleven hundred fifty-two of this article;

(b) Disclose the median and the mean number of days within which the data broker substantively responded to consumer deletion requests during the previous calendar year; and

(c) Disclose the metrics compiled pursuant to paragraphs (a) and (b) of this subdivision within the data broker's privacy policy posted on their internet website and accessible from a link included in the data broker's privacy policy.

2. In its disclosure pursuant to subdivision one of this section, a data broker shall disclose the number of consumer deletion requests that the data broker denied in whole or in part because of any of the following:

(a) The request was not verifiable;

(b) The request was not made by a consumer or a consumer's authorized agent;

(c) The request called for information exempt from deletion; or

(d) The request was denied on other grounds.

3. In its disclosure pursuant to subdivision one of this section, a data broker shall specify the number of consumer deletion requests in which deletion was not required in whole, or in part, under a relevant section of this article.

4. A data broker shall provide, in a form that is easily accessible to consumers, at least two or more designated methods for submitting deletion requests to such data broker directly. Such forms may include a toll-free telephone number, email or electronic submission via the data broker's internet website.

§ 1155. Data brokers; comprehensive information security program. 1. A data broker shall develop, implement, and maintain a documented comprehensive information security program that contains administrative, technical, and physical safeguards, including but not limited to the cessation of collection activities in the interest of the consumer, that are appropriate according to:

(a) the size, scope, and type of business of the data broker;

(b) the nature of resources available to the data broker;

(c) the volume and sensitivity of stored data; and

(d) the foreseeable risks of unauthorized access, use, or disclosure of personal information and sensitive personal information.

2. A comprehensive information security program required pursuant to subdivision one of this section shall include the following features:

(a) designation of one or more employees to maintain the program;

(b) identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper, or other records containing personal information;

(c) a process for evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including means of detecting and preventing security system failures;

(d) reasonable restrictions upon physical access to records containing personal information and storage of the records and data in locked facilities, storage areas, or containers;

(e) regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information and upgrading information safeguards as necessary to limit risks; and

(f) documentation of responsive actions taken in connection with any incident involving a breach of security and mandatory post-incident

review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

3. (a) A comprehensive information security program pursuant to subdivision one of this section shall, to the extent technically feasible, include the following technical elements:

(i) a secure user authentication protocol that has: (1) controlled management of user identifications and credentials; (2) secure methods of assigning and selecting passwords, or use of unique identifier technologies such as biometrics or token devices; (3) control of data passwords in a location, format and manner that does not compromise the security of the data protected; and (4) the ability to restrict access;

(ii) encryption and de-identification of all sensitive personal information transmitted across public networks or wirelessly prior to transmission;

(iii) reasonable monitoring of systems for unauthorized use of or access to personal information and sensitive personal information;

(iv) reasonably up-to-date firewall protection and operating system security patches that are reasonably designed to maintain the integrity of the personal information and sensitive personal information; and

(v) reasonably current system security software, including malware protection and up-to-date patches and virus definitions, configured to receive security updates on a regular basis.

(b) Nothing in this subdivision shall prohibit a comprehensive information security program from providing a higher degree of security than the protocols described in this subdivision.

§ 1156. Rulemaking. The attorney general shall adopt rules and regulations as necessary or convenient to implement and effectuate the provisions of this article.

§ 1157. Enforcement. 1. A data broker that fails to register under this article shall be subject to:

(a) a civil penalty of five hundred dollars for each day the data broker fails to register or fails to comply with the registration requirements as required by this article;

(b) a civil penalty equal to the amount of registration fees which would have been paid if the data broker had registered;

(c) a civil penalty of five hundred dollars for each deletion request for each day the data broker fails to delete information as required by section eleven hundred fifty-two of this article;

(d) a civil penalty of two hundred fifty dollars for each day the data broker fails to comply with the website disclosure requirements as set forth in section eleven hundred fifty-four of this article; and

(e) appropriate expenses incurred by the attorney general in the investigation and administration of the action, that are deemed appropriate by the court.

2. An application may be made by the attorney general in the name of the people of the state of New York to a court or justice having jurisdiction by a special proceeding to issue an injunction with respect to a violation of this article, and upon notice to the defendant of not less than five days, to enjoin and restrain the continuance of such violation.

§ 1158. Exemptions. 1. This article shall not apply to any of the following: (a) A covered entity 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 federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to

the extent the covered entity maintains, uses, and discloses protected health information in compliance with 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 federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the federal Health Information Technology for Economic and Clinical Health Act, Title XIII of the federal American Recovery and Reinvestment Act of 2009 (Public Law 111-5).

(b) A business associate of a covered entity governed by the privacy, security, and data 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 federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the federal Health Information Technology for Economic and Clinical Health Act, Title XIII of the federal American Recovery and Reinvestment Act of 2009 (Public Law 111-5), to the extent that such business associate maintains, uses, and discloses protected health information in compliance with 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 federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the federal Health Information Technology for Economic and Clinical Health Act, Title XIII of the federal American Recovery and Reinvestment Act of 2009 (Public Law 111-5).

(c) Information that is collected, used, or disclosed in research, as defined in Section 164.501 of Title 45 of the Code of Federal Regulations, including, but not limited to, a clinical trial, and that is conducted in accordance with applicable ethics, confidentiality, privacy, and security rules of Part 164 of Title 45 of the Code of Federal Regulations, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, good clinical practice guidelines issued by the International Council for Harmonization, or human subject protection requirements of the United States Food and Drug Administration.

(d) A health information network regulated under 10 NYCRR Part 300, including the department of health's designated contractor or a qualified entity under 10 NYCRR 300.4 to the extent such health information network is in compliance therewith with respect to the personal information.

(e) Personal information collected, processed, sold or disclosed to the extent that it is covered by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).

(f) Personal information collected, processed, sold, or disclosed to the extent that it is covered by the Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations.

(g) Personal information collected, processed, used, disclosed, sold, shared, licensed, or transferred by or on behalf of a candidate, a political committee, a party committee, a constituted committee, or an independent expenditure committee, as such terms are used in article fourteen of the election law, including an authorized committee as defined in section 14-200-a of the election law, or by a consultant, political, media or fundraising advisor, vendor, contractor, or agent that has been compensated, reimbursed or retained by, or that acts on behalf of or at the direction of, any such candidate or committee, to the extent that

such personal information is collected, processed, used, disclosed, sold, shared, licensed, or transferred solely in connection with activity regulated by the election law or to comply with a requirement of the election law.

2. For purposes of this section, the following terms shall have the following meanings:

(a) "Business associate" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(b) "Covered entity" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(c) "Identifiable private information" has the same meaning as defined in Section 46.102 of Title 45 of the Code of Federal Regulations.

(d) "Individually identifiable health information" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(e) "Protected health information" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

§ 2. Severability. If any clause, sentence, paragraph, subdivision, section or part of this act shall be adjudged by any court of competent jurisdiction to be invalid, such judgment shall not affect, impair, or invalidate the remainder thereof, but shall be confined in its operation to the clause, sentence, paragraph, subdivision, section or part thereof directly involved in the controversy in which such judgment shall have been rendered. It is hereby declared to be the intent of the legislature that this act would have been enacted even if such invalid provisions had not been included herein.

§ 3. This act shall take effect immediately.