

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.

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

6 6. "Consent" means any freely given, specific, informed, and unambig-
7 uous indication of a consumer's wishes by which such consumer, or such
8 consumer's legal guardian, a person who has power of attorney, or a
9 person acting as a conservator for such consumer, including by a state-
10 ment or by a clear affirmative action, signifies agreement to the proc-
11 essing of personal information relating to such consumer for a narrowly
12 defined particular purpose. Acceptance of a general or broad terms of
13 use, or similar document, that contains descriptions of personal infor-
14 mation processing along with other, unrelated information, shall not
15 constitute consent. Hovering over, muting, pausing, or closing a given
16 piece of content shall not constitute consent. Agreement obtained
17 through use of dark patterns shall not constitute consent.

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

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

24 (a) prohibits the contractor from:

25 (i) selling or sharing such personal information;

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

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

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

38 (b) includes a certification made by the contractor that the contrac-
39 tor understands the restrictions provided for in accordance with para-
40 graph (a) of this subdivision and will comply with them;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

37 (c) not attempt to reidentify such information, except that such busi-
38 ness may attempt to reidentify such information solely for the purpose
39 of determining whether its deidentification processes satisfy the
40 requirements of this subdivision; and

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

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

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

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

56 16. "Foreign actor" means either:

1 (a) the government of a foreign adversary country; or
2 (b) a partnership, association, corporation, organization, or other
3 combination of persons organized under the laws of or having its princi-
4 pal place of business in a foreign adversary country.

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

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

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

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

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

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

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

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

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

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

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

47 (v) biometric information;

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

52 (vii) geolocation data;

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

55 (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.

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

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

11 (a) information about a consumer searching for, accessing, procuring,
12 using, or otherwise interacting with goods or services associated with
13 the human reproductive system, which includes goods such as contracep-
14 tion including but not limited to condoms or birth-control pills, pre-
15 natal and fertility vitamins and supplements, menstrual-tracking apps,
16 and hormone-replacement therapy, and shall further include, but not be
17 limited to, services such as sperm- and egg-freezing, In Vitro Ferti-
18 lization, abortion care, vasectomies, sexual health counseling; treatment
19 or counseling for sexually transmitted infections, erectile dysfunction,
20 and reproductive tract infections; and precise geolocation information
21 about such treatments; or (b) information about a consumer's sexual
22 history and family planning, which includes information such consumer
23 inputs into a dating app about their history of sexually transmitted
24 infections or desire to have children.

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

26 (a) networks or information systems to detect security incidents that
27 compromise the availability, authenticity, integrity, and confidentiali-
28 ty of stored or transmitted personal information;

29 (b) businesses to detect security incidents, resist malicious, decep-
30 tive, fraudulent, or illegal actions and to help prosecute those respon-
31 sible for those actions; or

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

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

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

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

41 (1) disclose personal information; or

42 (2) interact with one or more third parties;

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

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

1 personal information, and comply with this article in all respects. A
2 third party shall not use or share the personal information of a consum-
3 er in a manner that is inconsistent with the promises made at the time
4 of collection. This subparagraph shall not authorize a business to make
5 retroactive privacy policy changes or make other changes in their priva-
6 cy policy.

7 33. "Sensitive personal information" means:

8 (a) personal information that reveals:

9 (i) a consumer's social security, driver's license, state identifica-
10 tion card, or passport number;

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

14 (iii) a consumer's precise geolocation;

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

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

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

20 (vii) reproductive health care data;

21 (viii) a consumer's genetic data; or

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

25 (b) the processing of biometric information for the purpose of unique-
26 ly identifying a consumer, including but not limited to:

27 (i) personal information collected and analyzed concerning a consum-
28 er's health; or

29 (ii) personal information collected and analyzed concerning a consum-
30 er's sex life or sexual orientation.

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

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

38 (i) selling or sharing such personal information;

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

45 (iii) retaining, using, or disclosing the information outside of the
46 direct business relationship between the service provider and such busi-
47 ness; or

48 (iv) combining such personal information that the service provider
49 receives from, or on behalf of, such business with personal information
50 that it receives from, or on behalf of, another person or persons, or
51 collects from its own interaction with the consumer. Such contract shall
52 permit the business to monitor such service provider's compliance with
53 such contract through measures, including, but not limited to, ongoing
54 manual reviews and automated scans and regular assessments, audits, or
55 other technical and operational testing at least once every twelve
56 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

1 (d) a processor to the business.

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

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

22 40. "Authorized agent" means:

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

24 (b) a parent or legal guardian that acts on behalf of the parent's
25 child or on behalf of a child for whom the guardian has legal responsi-
26 bility; or

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

30 § 1151. Registration of data brokers. 1. Each data broker shall:

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

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

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

39 (iii) Provide the following information to the attorney general in a
40 form and manner determined by the attorney general:

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

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

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

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

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

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

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

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

3 (H) whether the data broker collects or infers consumers' drivers'
4 license numbers, New York identification card numbers, tax identifica-
5 tion numbers, social security numbers, passport numbers, military iden-
6 tification numbers, or other unique identification numbers issued on a
7 government document commonly used to verify the identity of a specific
8 individual.

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

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

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

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

18 (M) whether the data broker collects or infers consumers' gender iden-
19 tity and gender expression data.

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

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

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

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

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

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

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

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

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

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

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

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

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

49 a. Deleting personal information.

50 b. Correcting inaccurate personal information.

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

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

55 e. Learning how to opt out of the sale or sharing of personal informa-
56 tion.

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

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

4 (Z) whether and to what extent the data broker or any of its subsid-
5 aries is regulated by any of the following:

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

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

10 (III) the privacy, security, and breach notification rules issued by
11 the United States Department of Health and Human Services, Parts 160 and
12 164 of Title 45 of the Code of Federal Regulations, established pursuant
13 to the federal Health Insurance Portability and Accountability Act of
14 1996 (Public Law 104-191); or

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

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

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

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

25 § 1152. Data deletion mechanism. 1. The attorney general shall estab-
26 lish a data deletion mechanism within one year of the effective date of
27 this section. Such data deletion mechanism shall:

28 (a) implement and maintain reasonable security procedures and prac-
29 tices, including, but not limited to, administrative, physical, and
30 technical safeguards appropriate to the nature of the information and
31 the purposes for which the personal information will be used and to
32 protect consumers' personal information from unauthorized use, disclo-
33 sure, access, destruction, or modification.

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

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

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

43 (e) allow a consumer to request the deletion of all personal informa-
44 tion related to that consumer through a single deletion request.

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

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

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

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

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

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

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

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

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

12 (o) provide a description of:

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

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

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

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

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

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

34 (b) cease all processing activities of personal information related to
35 the consumers making the verifiable consumer requests promptly and with-
36 out reasonable delay not to exceed five days after receiving a verifi-
37 able consumer request; and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

40 § 1153. Audit. Three years after the effective date of this section
41 and every three years thereafter, each data broker shall undergo an
42 audit by an independent third party to determine compliance with this
43 article. Each data broker shall submit a report resulting from the
44 audit written by such independent third party in a form determined by
45 the attorney general and any other materials required by the attorney
46 general to the attorney general within five business days of a written
47 request by the attorney general. Data brokers shall maintain such
48 reports and any required materials for at least six years.

49 § 1154. Data broker website disclosure requirements. 1. On or before
50 July first following each calendar year, or by such other date as the
51 attorney general may establish by regulation in which a business meets
52 the definition of a data broker as provided in this article, the busi-
53 ness shall clearly and conspicuously post their privacy policy on their
54 website as well as do all of the following:

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

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

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

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

12 (a) The request was not verifiable;

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

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

16 (d) The request was denied on other grounds.

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

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

26 § 1155. Data brokers; comprehensive information security program. 1. A
27 data broker shall develop, implement, and maintain a documented compre-
28 hensive information security program that contains administrative, tech-
29 anical, and physical safeguards, including but not limited to the cessa-
30 tion of collection activities in the interest of the consumer, that are
31 appropriate according to:

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

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

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

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

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

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

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

43 (c) a process for evaluating and improving, where necessary, the
44 effectiveness of the current safeguards for limiting such risks, includ-
45 ing means of detecting and preventing security system failures;

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

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

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

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

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

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

12 (ii) encryption and de-identification of all sensitive personal infor-
13 mation transmitted across public networks or wirelessly prior to trans-
14 mission;

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

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

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

23 (b) Nothing in this subdivision shall prohibit a comprehensive infor-
24 mation security program from providing a higher degree of security than
25 the protocols described in this subdivision.

26 § 1156. Rulemaking. The attorney general shall adopt rules and regu-
27 lations as necessary or convenient to implement and effectuate the
28 provisions of this article.

29 § 1157. Enforcement. 1. A data broker that fails to register under
30 this article shall be subject to:

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

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

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

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

42 (e) appropriate expenses incurred by the attorney general in the
43 investigation and administration of the action, that are deemed appro-
44 priate by the court.

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

51 § 1158. Exemptions. 1. This article shall not apply to any of the
52 following: (a) A covered entity governed by the privacy, security, and
53 breach notification rules issued by the United States Department of
54 Health and Human Services, Parts 160 and 164 of Title 45 of the Code of
55 Federal Regulations, established pursuant to the federal Health Insur-
56 ance Portability and Accountability Act of 1996 (Public Law 104-191), to

1 the extent the covered entity maintains, uses, and discloses protected
2 health information in compliance with the privacy, security, and breach
3 notification rules issued by the United States Department of Health and
4 Human Services, Parts 160 and 164 of Title 45 of the Code of Federal
5 Regulations, established pursuant to the federal Health Insurance Porta-
6 bility and Accountability Act of 1996 (Public Law 104-191) and the
7 federal Health Information Technology for Economic and Clinical Health
8 Act, Title XIII of the federal American Recovery and Reinvestment Act of
9 2009 (Public Law 111-5).

10 (b) A business associate of a covered entity governed by the privacy,
11 security, and data breach notification rules issued by the United States
12 Department of Health and Human Services, Parts 160 and 164 of Title 45
13 of the Code of Federal Regulations, established pursuant to the federal
14 Health Insurance Portability and Accountability Act of 1996 (Public Law
15 104-191) and the federal Health Information Technology for Economic and
16 Clinical Health Act, Title XIII of the federal American Recovery and
17 Reinvestment Act of 2009 (Public Law 111-5), to the extent that such
18 business associate maintains, uses, and discloses protected health
19 information in compliance with the privacy, security, and breach notifi-
20 cation rules issued by the United States Department of Health and Human
21 Services, Parts 160 and 164 of Title 45 of the Code of Federal Regu-
22 lations, established pursuant to the federal Health Insurance Portabil-
23 ity and Accountability Act of 1996 (Public Law 104-191) and the federal
24 Health Information Technology for Economic and Clinical Health Act,
25 Title XIII of the federal American Recovery and Reinvestment Act of 2009
26 (Public Law 111-5).

27 (c) Information that is collected, used, or disclosed in research, as
28 defined in Section 164.501 of Title 45 of the Code of Federal Regu-
29 lations, including, but not limited to, a clinical trial, and that is
30 conducted in accordance with applicable ethics, confidentiality, priva-
31 cy, and security rules of Part 164 of Title 45 of the Code of Federal
32 Regulations, the Federal Policy for the Protection of Human Subjects,
33 also known as the Common Rule, good clinical practice guidelines issued
34 by the International Council for Harmonization, or human subject
35 protection requirements of the United States Food and Drug Adminis-
36 tration.

37 (d) A health information network regulated under 10 NYCRR Part 300,
38 including the department of health's designated contractor or a quali-
39 fied entity under 10 NYCRR 300.4 to the extent such health information
40 network is in compliance therewith with respect to the personal informa-
41 tion.

42 (e) Personal information collected, processed, sold or disclosed to
43 the extent that it is covered by the federal Fair Credit Reporting Act
44 (15 U.S.C. Sec. 1681 et seq.).

45 (f) Personal information collected, processed, sold, or disclosed to
46 the extent that it is covered by the Gramm-Leach-Bliley Act (Public Law
47 106-102) and implementing regulations.

48 (g) Personal information collected, processed, used, disclosed, sold,
49 shared, licensed, or transferred by or on behalf of a candidate, a poli-
50 tical committee, a party committee, a constituted committee, or an inde-
51 pendent expenditure committee, as such terms are used in article four-
52 teen of the election law, including an authorized committee as defined
53 in section 14-200-a of the election law, or by a consultant, political,
54 media or fundraising advisor, vendor, contractor, or agent that has been
55 compensated, reimbursed or retained by, or that acts on behalf of or at
56 the direction of, any such candidate or committee, to the extent that

1 such personal information is collected, processed, used, disclosed,
2 sold, shared, licensed, or transferred solely in connection with activ-
3 ity regulated by the election law or to comply with a requirement of the
4 election law.

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

7 (a) "Business associate" has the same meaning as defined in Section
8 160.103 of Title 45 of the Code of Federal Regulations.

9 (b) "Covered entity" has the same meaning as defined in Section
10 160.103 of Title 45 of the Code of Federal Regulations.

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

13 (d) "Individually identifiable health information" has the same mean-
14 ing as defined in Section 160.103 of Title 45 of the Code of Federal
15 Regulations.

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

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

27 § 3. This act shall take effect immediately.