

STATE OF NEW YORK

7423--A

2023-2024 Regular Sessions

IN ASSEMBLY

May 19, 2023

Introduced by M. of A. ROZIC, D. ROSENTHAL, HEVESI -- 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 the management and oversight of personal data

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

1 Section 1. Short title. This act shall be known and may be cited as
2 the "New York data protection act".

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

16 2. This act seeks to help New York consumers regain their privacy. It
17 gives New York consumers the ability to exercise more control over their
18 personal data and requires businesses to be responsible, thoughtful, and
19 accountable managers of that information. To achieve this, this act
20 provides New York consumers a number of new rights, including clear
21 notice of how their data is being used, processed and shared; the abili-
22 ty to access and obtain a copy of their data in a commonly used elec-
23 tronic format, with the ability to transfer it between services; and the

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

LBD01642-10-3

ability to correct inaccurate data and to delete their data. This act also imposes obligations upon businesses to maintain reasonable data security for personal data, to notify New York consumers of foreseeable harms arising from use of their data and to obtain specific consent for that use, and to conduct regular assessments to ensure that data is not being used for unacceptable purposes. These data assessments can be obtained and evaluated by the New York State Attorney General, who is empowered to obtain penalties for violations of this act and prevent future violations.

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

ARTICLE 42

NEW YORK DATA PROTECTION ACT

Section 1100. Definitions.

1101. Jurisdictional scope.

1102. Consumer rights.

1103. Controller, processor, and third party responsibilities.

1104. Data brokers.

1105. Limitations.

1106. Enforcement.

1107. Miscellaneous.

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

1. "Biometric information" means any personal data generated from the measurement or specific technological processing of a natural person's biological, physical, or physiological characteristics that allows or confirms the unique identification of a natural person, including fingerprints, voice prints, iris or retina scans, facial scans or templates, and gait. "Biometric information" does not include a digital or physical photograph, an audio or video recording, or any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

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

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

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

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

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

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

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

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

11 8. "Decisions that produce legal or similarly significant effects"
12 means decisions made by the controller that result in the provision or
13 denial by the controller of financial or lending services, housing,
14 insurance, education enrollment or opportunity, criminal justice,
15 employment opportunities, health care services or access to essential
16 goods or services.

17 9. "Deidentified data" means data that cannot reasonably be used to
18 infer information about, or otherwise be linked to a particular consum-
19 er, household or device, provided that the processor or controller that
20 possesses the data:

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

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

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

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

34 11. "Genetic information" means any data, regardless of its format,
35 that concerns a consumer's genetic characteristics. "Genetic data"
36 includes but is not limited to (a) raw sequence data that result from
37 sequencing of a consumer's complete extracted or a portion of the
38 extracted deoxyribonucleic acid (DNA) information; (b) genotype and
39 phenotypic information that results from analyzing the raw sequence
40 data; and (c) self-reported health information that a consumer submits
41 to a company regarding the consumer's health conditions and that is used
42 for scientific research or product development and analyzed in
43 connection with the consumer's raw sequence data.

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

47 13. "Identified or identifiable" means a natural person who can be
48 identified, directly or indirectly, such as by reference to an identifi-
49 er such as a name, an identification number, location data, or an online
50 or device identifier.

51 14. "Natural person" means a natural person acting only in an individ-
52 ual or household context. It does not include a natural person known to
53 be acting in a professional or employment context.

54 15. "Person" means a natural person or a legal entity, including but
55 not limited to a proprietorship, partnership, limited partnership,
56 corporation, company, limited liability company or corporation, associ-

1 ation, or other firm or similar body, or any unit, division, agency,
2 department, or similar subdivision thereof.

3 16. "Personal data" means any data that identifies or could reasonably
4 be linked, directly or indirectly, with a specific natural person, or
5 household. Personal data does not include deidentified data, informa-
6 tion that is lawfully made publicly available from federal, state or
7 local government records, or information that a controller has a reason-
8 able basis to believe is lawfully made available to the general public
9 by the consumer or from widely distributed media.

10 17. "Precise geolocation data" means information derived from technol-
11 ogy, including, but not limited to, global position system level lati-
12 tude and longitude coordinates or other mechanisms, that directly iden-
13 tifies the specific location of an individual with precision and
14 accuracy within a radius of one thousand seven hundred fifty feet,
15 except as prescribed by regulations. Precise geolocation data does not
16 include the content of communications or any data generated by or
17 connected to advance utility metering infrastructure systems or equip-
18 ment for use by a utility.

19 18. "Process", "processes" or "processing" means an operation or set
20 of operations which are performed on data or on sets of data, including
21 but not limited to the collection, use, access, sharing, monetization,
22 analysis, retention, creation, generation, derivation, recording, organ-
23 ization, structuring, storage, disclosure, transmission, analysis,
24 disposal, licensing, destruction, deletion, modification, or deidenti-
25 cation of data.

26 19. "Processor" means a person that processes data on behalf of the
27 controller.

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

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

39 22. "Sale", "sell", or "sold" means the disclosure, transfer, convey-
40 ance, sharing, licensing, making available, processing, granting of
41 permission or authorization to process, or other exchange of personal
42 data, or providing access to personal data for monetary or other valu-
43 able consideration by the controller to a third party. "Sale" does not
44 include the following:

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

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

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

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

3 23. "Sensitive data" means personal data that reveals:

4 (a) racial or ethnic origin, religious beliefs, mental or physical
5 health condition or diagnosis, sex life, sexual orientation, or citizen-
6 ship or immigration status;

7 (b) genetic or biometric information for the purpose of uniquely iden-
8 tifying a natural person;

9 (c) precise geolocation data; or

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

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

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

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

29 § 1101. Jurisdictional scope. 1. This article applies to legal persons
30 that conduct business in New York or produce products or services that
31 are targeted to residents of New York, and that satisfy one or more of
32 the following thresholds:

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

34 (b) controls or processes personal data of fifty thousand consumers or
35 more; or

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

38 2. This article does not apply to:

39 (a) personal data processed by state and local governments, and munic-
40 ipal corporations, for processes other than sale (filing and processing
41 fees are not sale);

42 (b) a national securities association registered pursuant to section
43 15A of the Securities Exchange Act of 1934, as amended, or regulations
44 adopted thereunder or a registered futures association so designated
45 pursuant to section 17 of the Commodity Exchange Act, as amended, or any
46 regulations adopted thereunder;

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

53 (d) information that meets the following criteria:

54 (i) personal data collected, processed, sold, or disclosed pursuant to
55 and in compliance with the federal Gramm-Leach-Bliley act (P.L.
56 106-102), and implementing regulations;

1 (ii) personal data collected, processed, sold, or disclosed pursuant
2 to the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec.
3 2721 et seq.), if the collection, processing, sale, or disclosure is in
4 compliance with that law;

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

7 (iv) personal data collected, processed, sold, or disclosed pursuant
8 to the federal Farm Credit Act of 1971 (as amended in 12 U.S.C. Sec.
9 2001-2279cc) and its implementing regulations (12 C.F.R. Part 600 et
10 seq.) if the collection, processing, sale, or disclosure is in compli-
11 ance with that law;

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

13 (vi) data processed or maintained (A) in the course of an individual
14 applying to, employed by, or acting as an agent or independent contrac-
15 tor of a controller, processor or third party, to the extent that the
16 data is collected and used within the context of that role, (B) as the
17 emergency contact information of an individual under this section used
18 for emergency contact purposes, or (C) that is necessary to retain to
19 administer benefits for another individual relating to an individual
20 under clause (A) of this subparagraph and used for the purposes of
21 administering such benefits;

22 (vii) protected health information that is lawfully collected by a
23 covered entity or business associate and is governed by the privacy,
24 security, and breach notification rules issued by the United States
25 Department of Health and Human Services, Parts 160 and 164 of Title 45
26 of the Code of Federal Regulations, established pursuant to the Health
27 Insurance Portability and Accountability Act of 1996 (Public Law
28 104-191) ("HIPAA") and the Health Information Technology for Economic
29 and Clinical Health Act (Public Law 111-5);

30 (viii) patient identifying information for purposes of 42 C.F.R. Part
31 2, established pursuant to 42 U.S.C. Sec. 290dd-2, as long as such data
32 is not sold in violation of HIPAA or any state or federal law;

33 (ix) information and documents lawfully created for purposes of the
34 federal Health Care Quality Improvement Act of 1986, and related regu-
35 lations;

36 (x) patient safety work product created for purposes of 42 C.F.R. Part
37 3, established pursuant to 42 U.S.C. Sec. 299b-21 through 299b-26;

38 (xi) information that is treated in the same manner as information
39 exempt under subparagraph (vii) of this paragraph that is maintained by
40 a covered entity or business associate as defined by HIPAA or a program
41 or a qualified service organization as defined by 42 U.S.C. § 290dd-2,
42 as long as such data is not sold in violation of HIPAA or any state or
43 federal law;

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

46 (A) it is deidentified in accordance with the requirements for deiden-
47 tification set forth in Section 164.514 of Part 164 of Title 45 of the
48 Code of Federal Regulations;

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

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

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

10 (xiv) information maintained by a financial institution that is
11 subject to the Gramm-Leach-Bliley Act (Public Law 106-103), to the
12 extent the financial institution maintains the information in the same
13 manner as personal data as described in subparagraph (i) of this para-
14 graph;

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

21 (xvi) personal data processed only for one or more of the following
22 purposes:

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

25 (B) public health activities and purposes as described in Section
26 164.512 of Title 45 of the Code of Federal Regulations; and/or

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

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

33 (e) (i) an activity involving the collection, maintenance, disclosure,
34 sale, communication, or use of any personal data bearing on a consumer's
35 credit worthiness, credit standing, credit capacity, character, general
36 reputation, personal characteristics, or mode of living by a consumer
37 reporting agency, as defined in Title 15 U.S.C. Sec. 1681a(f), by a
38 furnisher of information, as set forth in Title 15 U.S.C. Sec. 1681s-2,
39 who provides information for use in a consumer report, as defined in
40 Title 15 U.S.C. Sec. 1861a(d), and by a user of a consumer report, as
41 set forth in Title 15 U.S.C. Sec. 1681b.; and

42 (ii) this paragraph shall apply only to the extent that such activity
43 involving the collection, maintenance, disclosure, sale, communication,
44 or use of such data by that agency, furnisher, or user is subject to
45 regulation under the Fair Credit Reporting Act, Title 15 U.S.C. Sec.
46 1681 et seq., and the data is not collected, maintained, used, communi-
47 cated, disclosed, or sold except as authorized by the Fair Credit
48 Reporting Act.

49 § 1102. Consumer rights. 1. Right to notice. (a) Notice. Each control-
50 ler that processes a consumer's personal data must make publicly and
51 consistently available, in a conspicuous and readily accessible manner,
52 a notice containing the following:

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

1 (ii) the categories of personal data processed by the controller and
2 by any processor who processes personal data on behalf of the control-
3 ler;

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

5 (iv) the purposes for processing personal data;

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

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

19 (b) Notice requirements.

20 (i) The notice must be written in easy-to-understand language and
21 format at an eighth grade reading level or below and in at least twelve
22 point font.

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

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

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

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

40 (i) targeted advertising;

41 (ii) the sale of personal data; and

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

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

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

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

1 (e) Controllers must treat user-enabled privacy controls in a browser,
2 browser plug-in, smartphone application, operating system, device
3 setting, or other mechanism that communicates or signals the consumer's
4 choice not to opt out of the processing of personal data in furtherance
5 of targeted advertising, or the sale of their personal data as an opt
6 out under this article. To the extent that the privacy control conflicts
7 with a consumer's consent, the controller shall comply with the privacy
8 control but may notify the consumer of such conflict and provide to such
9 consumer the choice to give controller specific consent to such process-
10 ing.

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

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

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

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

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

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

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

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

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

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

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

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

1 (d) Once a consumer has provided freely given, specific, informed, and
2 unambiguous opt-in consent to process their sensitive data for a proc-
3 essing purpose, a controller may rely on such consent until it is with-
4 drawn.

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

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

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

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

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

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

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

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

43 (ii) A controller shall not be prohibited from offering a different
44 price, rate, level, quality, or selection of goods or services to a
45 consumer, including offering goods or services for no fee, if the offer-
46 ing is in connection with a consumer's voluntary participation in bona
47 fide loyalty, rewards, premium features, discounts, or club card
48 program. If a consumer exercises their right pursuant to paragraph (a)
49 of subdivision two of this section, a controller may not sell personal
50 data to a third party controller as part of such a program unless: (A)
51 the sale is reasonably necessary to enable the third party to provide a
52 benefit to which the consumer is entitled; (B) the sale of personal data
53 to third parties is clearly disclosed in the terms of the program; and
54 (C) the third party uses the personal data only for purposes of facili-
55 tating such a benefit to which the consumer is entitled and does not

1 retain or otherwise use or disclose the personal data for any other
2 purpose.

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

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

16 4. Right to access. Upon the verified request of a consumer, a
17 controller shall:

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

22 (b) provide the category of each processor or third party to whom the
23 controller disclosed, transferred, or sold the consumer's personal data
24 and, for each category of processor or third party, (i) the categories
25 of the consumer's personal data disclosed, transferred, or sold to each
26 processor or third party and (ii) the purposes for which each category
27 of the consumer's personal data was disclosed, transferred, or sold to
28 each processor or third party.

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

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

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

54 (c) If, after any investigation under paragraph (a) of this subdivi-
55 sion of any personal data disputed by a consumer, an item of the

1 personal data is found to be inaccurate or incomplete, or cannot be
2 verified, the controller must:

3 (i) correct the inaccurate or incomplete personal data of the consum-
4 er; and

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

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

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

21 (i) within forty-five days after receiving the verified request,
22 delete any or all of the consumer's personal data, as directed by the
23 consumer or their agent, that the controller possesses or controls; and

24 (ii) unless it proves impossible or involves disproportionate effort
25 that is documented in writing by the controller, communicate such
26 request to each third party to whom the controller disclosed, trans-
27 ferred or sold the personal data within one year preceding the consum-
28 er's request and to require those third parties to do the same for any
29 further third parties they disclosed, transferred, or sold the personal
30 data to.

31 (b) For personal data that is not possessed by the controller but by a
32 processor of the controller, the controller may choose to (i) communi-
33 cate the consumer's request for deletion to the processor, or (ii)
34 request that the processor return to the controller the personal data
35 that is the subject of the consumer's request and delete such personal
36 data upon receipt of the request.

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

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

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

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

52 (ii) it is necessary for the controller to maintain the consumer's
53 personal data to engage in public or peer-reviewed scientific, histor-
54 ical, or statistical research in the public interest that adheres to all
55 other applicable ethics and privacy laws, when the controller's deletion
56 of the information is likely to render impossible or seriously impair

1 the achievement of such research, provided that the consumer has given
2 informed consent and the personal data is not processed for any purpose
3 other than such research.

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

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

17 (b) A controller shall permit the exercise of rights and carry out its
18 obligations set forth in subdivisions four through seven of this section
19 free of charge, at least twice annually to the consumer. Where requests
20 from a consumer are manifestly unfounded or excessive, in particular
21 because of their repetitive character, the controller may either (i)
22 charge a reasonable fee to cover the administrative costs of complying
23 with the request or (ii) refuse to act on the request and notify the
24 consumer of the reason for refusing the request. The controller bears
25 the burden of demonstrating the manifestly unfounded or excessive char-
26 acter of the request.

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

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

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

51 9. Implementation of rights. Controllers must provide easily accessi-
52 ble and convenient means for consumers to exercise their rights under
53 this article.

54 10. Non-waiver of rights. Any provision of a contract or agreement of
55 any kind that purports to waive or limit in any way a consumer's rights

1 under this article is contrary to public policy and is void and unen-
2 forceable.

3 § 1103. Controller, processor, and third party responsibilities. 1.
4 Controller responsibilities. (a) Data protection assessments. (i) A
5 controller shall regularly conduct and document a data protection
6 assessment for each of the controller's processing activities that
7 presents a heightened risk of harm to a consumer. For the purposes of
8 this section, processing that presents a heightened risk of harm to a
9 consumer includes: (A) the processing of personal data for the purposes
10 of targeting advertising, (B) the sale of personal data, (C) the proc-
11 essing of personal data for the purposes of profiling, where such
12 profiling presents a reasonably foreseeable risk of (I) unfair or decep-
13 tive treatment of, or unlawful disparate impact on consumers, (II)
14 financial, physical or reputational injury to consumers, (III) a phys-
15 ical or other intrusion upon the solitude or seclusion, or the private
16 affairs or concerns of consumers where such intrusion would be offensive
17 to a reasonable person, or (IV) other substantial injury to consumers;
18 and (D) the processing of sensitive data.

19 (ii) Data protection assessments conducted pursuant to subparagraph
20 (i) of this paragraph shall identify and weigh the benefits that may
21 flow, directly and indirectly, from the processing to the controller,
22 the consumer, other stakeholders and the public against the potential
23 risks to the rights of the consumer associated with such processing, as
24 mitigated by safeguards that can be employed by the controller to reduce
25 such risks. The controller shall factor into any such data protection
26 assessment that use of deidentified data and the reasonable expectations
27 of consumers, as well as the context of the processing and the relation-
28 ship between the controller and the consumer whose personal data will be
29 processed.

30 (iii) The attorney general may require that a controller disclose any
31 data protection assessment that is relevant to an investigation
32 conducted by the attorney general, and the controller shall make the
33 data protection assessment available to the attorney general. The attor-
34 ney general may evaluate the data protection assessment to assess
35 compliance with the provisions of this article. Data protection assess-
36 ments shall be confidential and shall be exempt from disclosure under
37 the freedom of information law. To the extent any information contained
38 in a data protection assessment disclosure to the attorney general
39 includes information subject to attorney-client privilege or work prod-
40 uct protection, such disclosure shall not constitute a waiver of such
41 privilege or protection.

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

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

50 (vi) Data protection assessment requirements shall apply to processing
51 activities created or generated after the effective date of this arti-
52 cle.

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

1 (i) designing a user interface with the purpose or substantial effect
2 of deceiving consumers, obscuring consumers' rights under this article,
3 or subverting or impairing user autonomy, decision-making, or choice; or
4 (ii) obtaining consent in a manner designed to overpower a consumer's
5 resistance; for example, by making excessive requests for consent.

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

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

17 (ii) At least annually, a controller shall review its retention prac-
18 tices for the purpose of ensuring that it is maintaining the minimum
19 amount of personal data as is necessary for the operation of its busi-
20 ness. A controller must securely dispose of all personal data that is no
21 longer (A) necessary to provide the services or goods requested by the
22 consumer, (B) necessary for the internal business operations of the
23 controller and consistent with the disclosures made to the consumer
24 pursuant to section eleven hundred two of this article, or (C) necessary
25 to comply with the legal obligations of the controller.

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

29 (I) denying services or goods to consumers;

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

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

37 (B) A controller shall not be prohibited from offering a different
38 price, rate, level, quality, or selection of goods or services to a
39 consumer, including offering goods or services for no fee, if the offer-
40 ing is in connection with a consumer's voluntary participation in bona
41 fide loyalty, rewards, premium features, discounts, or club card
42 program. If a consumer exercises their right pursuant to paragraph (a)
43 of subdivision two of section eleven hundred two of this article, a
44 controller may not sell personal data to a third party controller as
45 part of such a program unless: (I) the sale is reasonably necessary to
46 enable the third party to provide a benefit to which the consumer is
47 entitled; (II) the sale of personal data to third parties is clearly
48 disclosed in the terms of the program; and (III) the third party uses
49 the personal data only for purposes of facilitating such a benefit to
50 which the consumer is entitled and does not retain or otherwise use or
51 disclose the personal data for any other purpose.

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

55 (f) Agreements with processors. (i) Before making any disclosure,
56 transfer, or sale of personal data to any processor, the controller must

1 enter into a written, signed contract with that processor. Such contract
2 must be binding and clearly set forth instructions for processing data,
3 the nature and purpose of processing, the type of data subject to proc-
4 essing, the duration of processing, and the rights and obligations of
5 both parties. The contract must also include requirements that the
6 processor must:

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

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

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

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

20 (E) comply with any exercises of a consumer's rights under section
21 eleven hundred two of this article upon the request of the controller,
22 subject to the limitations set forth in section eleven hundred five of
23 this article;

24 (F) at the controller's direction, delete or return all personal data
25 to the controller as requested at the end of the provision of services,
26 unless retention of the personal data is required by law;

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

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

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

42 (J) engage any further processor pursuant to a written, signed
43 contract that includes the contractual requirements provided in this
44 paragraph, containing at minimum the same obligations that the processor
45 has entered into with regard to the data.

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

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

1 (iv) Determining whether a person is acting as a controller or proces-
2 sor with respect to a specific processing of data is a fact-based deter-
3 mination that depends upon the context in which personal data is to be
4 processed. A processor that continues to adhere to a controller's
5 instructions with respect to a specific processing of personal data
6 remains a processor.

7 (g) Third parties. (i) A controller must not share, disclose, trans-
8 fer, or sell personal data, or facilitate or enable the processing,
9 disclosure, transfer, or sale to a third party of personal data for
10 which a consumer has exercised their opt-out rights pursuant to subdivi-
11 sion two of section eleven hundred two of this article, or for which
12 consent of the consumer pursuant to subdivision three of section eleven
13 hundred two of this article, has not been obtained or is not currently
14 in effect. Any request for consent to share, disclose, transfer, or sell
15 personal data, or to facilitate or enable the processing, disclosure,
16 transfer, or sale of personal data to a third party of personal data to
17 a third party must clearly include the category of the third party and
18 the processing purposes for which the third party may use the personal
19 data.

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

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

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

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

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

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

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

55 (c) Processors shall be under a continuing obligation to engage in
56 reasonable measures to review their activities for circumstances that

1 may have altered their ability to identify a specific natural person and
2 to update their classifications of data as identified or identifiable
3 accordingly.

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

7 (e) A processor must adopt appropriate technical and organizational
8 measures to assist a controller in fulfilling the controller's obli-
9 gation to respond to consumer requests to exercise their rights pursuant
10 to section eleven hundred two of this article, taking into account the
11 nature of the processing and the information available to the processor.

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

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

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

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

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

25 (a) The processing is required by law;

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

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

30 § 1104. Data brokers. 1. A data broker, as defined under this article,
31 must annually, on or before January thirty-first following a year in
32 which a person meets the definition of data broker in this article:

33 (a) Register with the attorney general;

34 (b) 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 (c) Provide the following information:

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

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

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

47 (iv) a statement whether the data broker implements a purchaser
48 credentialing process; and

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

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

53 (a) annually, on or before January thirty-first following a year in
54 which a person meets the definition of controller in this act, provide
55 to the attorney general a list of all data brokers or persons reasonably

1 believed to be data brokers to which the controller provided personal
2 data in the preceding year; and

3 (b) not sell a consumer's personal data to an entity reasonably
4 believed to be a data broker that is not registered with the attorney
5 general.

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

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

23 § 1105. Limitations. 1. This article does not require a controller or
24 processor to do any of the following solely for purposes of complying
25 with this article:

26 (a) Reidentify deidentified data;

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

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

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

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

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

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

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

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

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

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

4 (e) Prevent, detect, protect against, or respond to security inci-
5 dents, identity theft, fraud, harassment, malicious or deceptive activ-
6 ities, or any illegal activity; preserve the integrity or security of
7 systems; or investigate, report, or prosecute those responsible for any
8 such action;

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

11 (g) Process business contact information, including a natural person's
12 name, position name or title, business telephone number, business
13 address, business electronic mail address, business fax number, or qual-
14 ifications and any other similar information about the natural person.

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

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

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

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

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

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

37 § 1106. Enforcement. 1. Whenever it appears to the attorney general,
38 either upon complaint or otherwise, that any person or persons has
39 engaged in or is about to engage in any of the acts or practices stated
40 to be unlawful under this article, the attorney general may bring an
41 action or special proceeding in the name and on behalf of the people of
42 the state of New York to enjoin any violation of this article, to obtain
43 restitution of any moneys or property obtained directly or indirectly by
44 any such violation, to obtain disgorgement of any profits obtained
45 directly or indirectly by any such violation, to obtain civil penalties
46 of not more than twenty thousand dollars per violation, and to obtain
47 any such other and further relief as the court may deem proper, includ-
48 ing preliminary relief.

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

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

1 (c) In assessing the amount of penalties, the court must consider any
2 one or more of the relevant circumstances presented by any of the
3 parties, including, but not limited to, the nature and seriousness of
4 the misconduct, the number of violations, the persistence of the miscon-
5 duct, the length of time over which the misconduct occurred, the will-
6 fulness of the violator's misconduct, and the violator's financial
7 condition.

8 2. In connection with any proposed action or special proceeding under
9 this section, the attorney general is authorized to take proof and make
10 a determination of the relevant facts, and to issue subpoenas in accord-
11 ance with the civil practice law and rules. The attorney general may
12 also require such other data and information as he or she may deem rele-
13 vant and may require written responses to questions under oath. Such
14 power of subpoena and examination shall not abate or terminate by reason
15 of any action or special proceeding brought by the attorney general
16 under this article.

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

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

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

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

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

41 § 1107. Miscellaneous. 1. Preemption: This article preempts the laws,
42 ordinances, regulations, or the equivalent adopted by any local entity
43 regarding the processing, collection, transfer, disclosure, and sale of
44 consumers' personal data by a controller or processor subject to this
45 article.

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

55 3. Regulatory authority: (a) The attorney general is hereby authorized
56 and empowered to adopt, promulgate, amend and rescind suitable rules and

1 regulations to carry out the provisions of this article, including rules
2 governing the form and content of any disclosures or communications
3 required by this article.

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

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

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

26 § 5. This act shall take effect immediately; provided, however, that
27 sections 1101, 1102, 1103, 1105, 1106 and 1107 of the general business
28 law, as added by section three of this act, shall take effect two years
29 after it shall have become a law.