

STATE OF NEW YORK

365

2023-2024 Regular Sessions

IN SENATE

(Prefiled)

January 4, 2023

Introduced by Sens. THOMAS, COMRIE, JACKSON, KRUEGER, MAY, RAMOS -- read twice and ordered printed, and when printed to be committed to the Committee on Consumer Protection

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 privacy 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; the

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

LBD01642-01-3

ability to correct inaccurate data and to delete their data; and the ability to challenge certain automated decisions. This act also imposes obligations upon businesses to maintain reasonable data security for personal data, to notify New York consumers of foreseeable harms arising from use of their data and to obtain specific consent for that use, and to conduct regular assessments to ensure that data is not being used for unacceptable purposes. These data assessments can be obtained and evaluated by the New York State Attorney General, who is empowered to obtain penalties for violations of this act and prevent future violations. This act also grants New York consumers who have been injured as the result of a violation a private right of action, which includes reasonable attorneys' fees to a prevailing plaintiff.

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

ARTICLE 42

NEW YORK PRIVACY ACT

Section 1100. Definitions.

1101. Jurisdictional scope.

1102. Consumer rights.

1103. Controller, processor, and third party responsibilities.

1104. Data brokers.

1105. Limitations.

1106. Enforcement and private right of action.

1107. Miscellaneous.

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

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

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

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

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

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

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

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

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

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

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

16 9. "Decisions that produce legal or similarly significant effects"
17 means decisions made by the controller that result in the provision or
18 denial by the controller of financial or lending services, housing,
19 insurance, education enrollment or opportunity, criminal justice,
20 employment opportunities, health care services or access to essential
21 goods or services.

22 10. "Deidentified data" means data that cannot reasonably be used to
23 infer information about, or otherwise be linked to a particular consum-
24 er, household or device, provided that the processor or controller that
25 possesses the data:

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

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

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

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

39 12. "Identified or identifiable" means a natural person who can be
40 identified, directly or indirectly, such as by reference to an identifi-
41 er such as a name, an identification number, location data, or an online
42 or device identifier.

43 13. "Meaningful human review" means review or oversight by one or more
44 individuals who (a) are trained in the capabilities and limitations of
45 the algorithm at issue and the procedures to interpret and act on the
46 output of the algorithm, and (b) have the authority to alter the auto-
47 mated decision under review.

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

51 15. "Person" means a natural person or a legal entity, including but
52 not limited to a proprietorship, partnership, limited partnership,
53 corporation, company, limited liability company or corporation, associ-
54 ation, or other firm or similar body, or any unit, division, agency,
55 department, or similar subdivision thereof.

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

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

13 18. "Process", "processes" or "processing" means an operation or set
14 of operations which are performed on data or on sets of data, including
15 but not limited to the collection, use, access, sharing, monetization,
16 analysis, retention, creation, generation, derivation, recording, organ-
17 ization, structuring, storage, disclosure, transmission, analysis,
18 disposal, licensing, destruction, deletion, modification, or deidentifi-
19 cation of data.

20 19. "Processor" means a person that processes data on behalf of the
21 controller.

22 20. "Profiling" means any form of automated processing performed on
23 personal data to evaluate, analyze, or predict personal aspects related
24 to an identified or identifiable natural person's economic situation,
25 health, personal preferences, interests, reliability, behavior,
26 location, or movements. Profiling does not include evaluation, analy-
27 sis, or prediction based solely upon a natural person's current search
28 query or current visit to a website or online application, if no
29 personal data is retained after the completion of the activity for the
30 purposes identified in this subdivision.

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

34 22. "Sale", "sell", or "sold" means the disclosure, transfer, convey-
35 ance, sharing, licensing, making available, processing, granting of
36 permission or authorization to process, or other exchange of personal
37 data, or providing access to personal data for monetary or other valu-
38 able consideration by the controller to a third party. "Sale" includes
39 enabling, facilitating or providing access to personal data for targeted
40 advertising. "Sale" does not include the following:

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

44 (b) the disclosure or transfer of data as an asset that is part of a
45 merger, acquisition, bankruptcy, or other transaction in which another
46 entity assumes control or ownership of all or a majority of the control-
47 ler's assets.

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

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

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

54 (c) precise geolocation data.

55 24. "Targeted advertising" means advertising based upon profiling.

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

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

11 § 1101. Jurisdictional scope. 1. This article applies to legal persons
12 that conduct business in New York or produce products or services that
13 are targeted to residents of New York, and that satisfy one or more of
14 the following thresholds:

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

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

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

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

24 2. This article does not apply to:

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

28 (b) a national securities association registered pursuant to section
29 15A of the Securities Exchange Act of 1934, as amended, or regulations
30 adopted thereunder or a registered futures association so designated
31 pursuant to section 17 of the Commodity Exchange Act, as amended, or any
32 regulations adopted thereunder;

33 (c) information that meets the following criteria:

34 (i) personal data collected, processed, sold, or disclosed pursuant to
35 and in compliance with the federal Gramm-Leach-Bliley act (P.L.
36 106-102), and implementing regulations;

37 (ii) personal data collected, processed, sold, or disclosed pursuant
38 to the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec.
39 2721 et seq.), if the collection, processing, sale, or disclosure is in
40 compliance with that law;

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

43 (iv) personal data collected, processed, sold, or disclosed pursuant
44 to the federal Farm Credit Act of 1971 (as amended in 12 U.S.C. Sec.
45 2001-2279cc) and its implementing regulations (12 C.F.R. Part 600 et
46 seq.) if the collection, processing, sale, or disclosure is in compli-
47 ance with that law;

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

49 (vi) data maintained as employment records, for purposes other than
50 sale;

51 (vii) protected health information that is lawfully collected by a
52 covered entity or business associate and is governed by the privacy,
53 security, and breach notification rules issued by the United States
54 Department of Health and Human Services, Parts 160 and 164 of Title 45
55 of the Code of Federal Regulations, established pursuant to the Health
56 Insurance Portability and Accountability Act of 1996 (Public Law

104-191) ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5);

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(d) (i) an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal data bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in Title 15 U.S.C. Sec. 1681a(f), by a

furnisher of information, as set forth in Title 15 U.S.C. Sec. 1681s-2, who provides information for use in a consumer report, as defined in Title 15 U.S.C. Sec. 1861a(d), and by a user of a consumer report, as set forth in Title 15 U.S.C. Sec. 1681b.; and

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

§ 1102. Consumer rights. 1. Right to notice. (a) Notice. Each controller that processes a consumer's personal data must make publicly and persistently available, in a conspicuous and readily accessible manner, a notice containing the following:

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

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

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

(iv) the purposes for processing personal data;

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

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

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

(b) Notice requirements.

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

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

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

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

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

4 (i) targeted advertising;
5 (ii) the sale of personal data; and
6 (iii) profiling in furtherance of decisions that produce legal or
7 similarly significant effects concerning a consumer.

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

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

14 (d) A controller must not request that a consumer who has opted out of
15 certain purposes of processing personal data opt back in, unless those
16 purposes subsequently become necessary to provide the services or goods
17 requested by a consumer. Targeted advertising and sale of personal data
18 shall not be considered processing purposes that are necessary to
19 provide service or goods requested by a consumer.

20 (e) Controllers must treat user-enabled privacy controls in a browser,
21 browser plug-in, smartphone application, operating system, device
22 setting, or other mechanism that communicates or signals the consumer's
23 choice not to opt out of the processing of personal data in furtherance
24 of targeted advertising, the sale of their personal data, or profiling
25 in furtherance of decisions that produce legal or similarly significant
26 effects concerning the consumer as an opt out under this article. To the
27 extent that the privacy control conflicts with a consumer's consent, the
28 privacy control settings govern, unless the consumer provides freely
29 given, specific, informed, and unambiguous consent to override the
30 privacy control.

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

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

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

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

46 (i) include a clear and conspicuous description of each category of
47 data and processing purpose for which consent is sought;

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

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

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

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

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

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

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

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

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

30 (g) Controllers must not request consent from a consumer who has
31 previously withheld or denied consent to process sensitive data, unless
32 consent is necessary to provide the services or goods requested by the
33 consumer.

34 (h) Controllers must treat user-enabled privacy controllers in a brow-
35 ser, browser plug-in, smartphone application, operating system, device
36 setting, or other mechanism that communicates or signals the consumer's
37 choices to opt out of the processing of personal data in furtherance of
38 targeted advertising, the sale of their personal data, or profiling in
39 furtherance of decisions that produce legal or similarly significant
40 effects concerning the consumer as a denial of consent to process sensi-
41 tive data under this article. To the extent that the privacy control
42 conflicts with a consumer's consent, the privacy control settings
43 govern, unless the consumer provides freely given, specific, informed,
44 and unambiguous opt-in consent to override the privacy control.

45 (i) A controller must not discriminate against a consumer for with-
46 holding or denying consent, including, but not limited to, by:

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

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

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

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

8 (k) In the event of a merger, acquisition, bankruptcy, or other trans-
9 action in which another entity assumes control or ownership of all or
10 majority of the controller's assets, any consent provided to the
11 controller by a consumer prior to such transaction shall be deemed with-
12 drawn.

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

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

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

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

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

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

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

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

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

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

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

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

20 (ii) unless it proves impossible or involves disproportionate effort
21 that is documented in writing by the controller, communicate such
22 request to each processor or third party to whom the controller
23 disclosed, transferred or sold the personal data within one year preced-
24 ing the consumer's request and to require those processors or third
25 parties to do the same for any further processors or third parties they
26 disclosed, transferred, or sold the personal data to.

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

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

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

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

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

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

1 8. Automated decision-making. (a) Whenever a controller makes an auto-
2 mated decision involving solely automated processing that materially
3 contributes to a denial of financial or lending services, housing,
4 public accommodation, insurance, health care services, or access to
5 basic necessities, such as food and water, or produces legal or similar-
6 ly significant effects the controller must:

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

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

13 (iii) explain the process to appeal the decision.

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

20 (c) (i) A controller or processor engaged in automated decision-making
21 affecting financial or lending services, housing, public accommodation,
22 insurance, education enrollment, employment, health care services, or
23 access to basic necessities, such as food and water, or producing legal
24 or other similarly significant effects or engaged in assisting others in
25 automated decision-making in those fields, must annually conduct an
26 impact assessment of such automated decision-making that:

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

32 (B) assesses whether the automated decision-making system produces
33 discriminatory results on the basis of a consumer's or class of consum-
34 ers' actual or perceived race, color, ethnicity, religion, national
35 origin, sex, gender, gender identity, sexual orientation, familial
36 status, biometric information, lawful source of income, or disability
37 and outlines mitigations for any identified performance differences
38 across relevant groups impacted by the system. Such evaluations should
39 be conducted on a system prior to deployment, including in the environ-
40 ment in which a system is going to be used, and throughout the lifecycle
41 of a system.

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

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

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

52 9. Responding to requests. (a) A controller must take action under
53 subdivisions four through seven of this section and inform the consumer
54 of any actions taken without undue delay and in any event within forty-
55 five days of receipt of the request. That period may be extended once by
56 forty-five additional days where reasonably necessary, taking into

1 account the complexity and number of the requests. The controller must
2 inform the consumer of any such extension within forty-five days of
3 receipt of the request, together with the reasons for the delay. When a
4 controller denies any such request, it must within this period disclose
5 to the consumer a statement in writing of the specific reasons for the
6 denial.

7 (b) A controller shall permit the exercise of rights and carry out its
8 obligations set forth in subdivisions four through seven of this section
9 free of charge, at least twice annually to the consumer. Where requests
10 from a consumer are manifestly unfounded or excessive, in particular
11 because of their repetitive character, the controller may either (i)
12 charge a reasonable fee to cover the administrative costs of complying
13 with the request or (ii) refuse to act on the request and notify the
14 consumer of the reason for refusing the request. The controller bears
15 the burden of demonstrating the manifestly unfounded or excessive char-
16 acter of the request.

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

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

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

41 10. Implementation of rights. Controllers must provide easily accessi-
42 ble and convenient means for consumers to exercise their rights under
43 this article.

44 11. Non-waiver of rights. Any provision of a contract or agreement of
45 any kind that purports to waive or limit in any way a consumer's rights
46 under this article is contrary to public policy and is void and unen-
47 forceable.

48 § 1103. Controller, processor, and third party responsibilities. 1.
49 Controller responsibilities. (a) Data protection assessment. A control-
50 ler shall regularly conduct and document a data protection assessment
51 for processing activities that present a heightened risk of harm to the
52 consumer. Such assessment must identify and weigh the benefits that may
53 flow, directly and indirectly, from the processing to the controller,
54 the consumer, other stakeholders, and the public against the potential
55 risks to the rights of the consumer, or class of consumers, associated
56 with the processing, as mitigated by safeguards that the controller can

employ to reduce the risks. The controller shall factor into this assessment the use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, with the goal of restricting or prohibiting such processing if the risks of harm to the consumer outweigh the benefits resulting from the processing to the consumer. Processing that presents a heightened risk of harm to the consumer includes the following:

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

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

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

(iv) sale of personal data;

(v) processing sensitive data; and

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

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

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

(C) a physical or otherwise intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or

(D) other substantial injury to consumers.

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

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

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

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

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

(B) Risk assessments must assess at a minimum:

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

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

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

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

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

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

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

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

12 (iii) (A) A controller shall limit the use and retention of a consum-
13 er's personal data to what is (I) necessary to provide the services or
14 goods requested by the consumer, (II) necessary for the internal busi-
15 ness operations of the controller and consistent with the disclosures
16 made to the consumer pursuant to section eleven hundred two of this
17 article, or (III) necessary to comply with the legal obligations of the
18 controller.

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

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

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

36 (A) denying services or goods to consumers;

37 (B) charging different prices for services or goods, 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 services or goods or a different level or quality of services
42 or goods.

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

46 (e) Agreements with processors. (i) Before making any disclosure,
47 transfer, or sale of personal data to any processor, the controller must
48 enter into a written, signed contract with that processor. Such contract
49 must be binding and clearly set forth instructions for processing data,
50 the nature and purpose of processing, the type of data subject to proc-
51 essing, the duration of processing, and the rights and obligations of
52 both parties. The contract must also include requirements that the
53 processor must:

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

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

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

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

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

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

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

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

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

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

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

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

49 (iv) Determining whether a person is acting as a controller or proces-
50 sor with respect to a specific processing of data is a fact-based deter-
51 mination that depends upon the context in which personal data is to be
52 processed. A processor that continues to adhere to a controller's
53 instructions with respect to a specific processing of personal data
54 remains a processor.

55 (f) Third parties. (i) A controller must not share, disclose, trans-
56 fer, or sell personal data, or facilitate or enable the processing,

1 disclosure, transfer, or sale to a third party of personal data for
2 which a consumer has exercised their opt-out rights pursuant to subdivi-
3 sion two of section eleven hundred two of this article, or for which
4 consent of the consumer pursuant to subdivision three of section eleven
5 hundred two of this article, has not been obtained or is not currently
6 in effect. Any request for consent to share, disclose, transfer, or sell
7 personal data, or to facilitate or enable the processing, disclosure,
8 transfer, or sale of personal data to a third party of personal data to
9 a third party must clearly include the category of the third party and
10 the processing purposes for which the third party may use the personal
11 data.

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

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

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

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

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

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

43 (b) A processor is not required to comply with a request by the
44 consumer submitted pursuant to this article by a consumer directly to
45 the processor to the extent that the processor has processed the consum-
46 er's personal data solely in its role as a processor for a controller.

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

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

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

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

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

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

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

14 (a) The processing is required by law;

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

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

19 § 1104. Data brokers. 1. A data broker, as defined under this article,
20 must:

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

23 (i) Register with the attorney general;

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

29 (iii) Provide the following information:

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

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

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

37 (D) a statement whether the data broker implements a purchaser creden-
38 tialing process; and

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

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

43 (a) annually, on or before January thirty-first following a year in
44 which a person meets the definition of controller in this act, provide
45 to the attorney general a list of all data brokers or persons reasonably
46 believed to be data brokers to which the controller provided personal
47 data in the preceding year; and

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

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

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

12 § 1105. Limitations. 1. This article does not require a controller or
13 processor to do any of the following solely for purposes of complying
14 with this article:

15 (a) Reidentify deidentified data;

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

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

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

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

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

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

35 (a) Comply with federal, state, or local laws, rules, or regulations;

36 (b) Comply with a civil, criminal, or regulatory inquiry, investi-
37 gation, subpoena, or summons by federal, state, local, or other govern-
38 mental authorities;

39 (c) Cooperate with law enforcement agencies concerning conduct or
40 activity that the controller or processor reasonably and in good faith
41 believes may violate federal, state, or local laws, rules, or regu-
42 lations;

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

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

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

52 (g) Prevent, detect, protect against, or respond to security inci-
53 dents, identity theft, fraud, harassment, malicious or deceptive activi-
54 ties, or any illegal activity; preserve the integrity or security of
55 systems; or investigate, report, or prosecute those responsible for any
56 such action;

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

3 (i) Process business contact information, including a natural person's
4 name, position name or title, business telephone number, business
5 address, business electronic mail address, business fax number, or qual-
6 ifications and any other similar information about the natural person.

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

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

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

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

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

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

29 § 1106. Enforcement and private right of action. 1. Whenever it
30 appears to the attorney general, either upon complaint or otherwise,
31 that any person or persons has engaged in or is about to engage in any
32 of the acts or practices stated to be unlawful under this article, the
33 attorney general may bring an action or special proceeding in the name
34 and on behalf of the people of the state of New York to enjoin any
35 violation of this article, to obtain restitution of any moneys or prop-
36 erty obtained directly or indirectly by any such violation, to obtain
37 disgorgement of any profits obtained directly or indirectly by any such
38 violation, to obtain civil penalties of not more than fifteen thousand
39 dollars per violation, and to obtain any such other and further relief
40 as the court may deem proper, including preliminary relief.

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

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

48 (c) In assessing the amount of penalties, the court must consider any
49 one or more of the relevant circumstances presented by any of the
50 parties, including, but not limited to, the nature and seriousness of
51 the misconduct, the number of violations, the persistence of the miscon-
52 duct, the length of time over which the misconduct occurred, the will-
53 fulness of the violator's misconduct, and the violator's financial
54 condition.

55 2. In connection with any proposed action or special proceeding under
56 this section, the attorney general is authorized to take proof and make

1 a determination of the relevant facts, and to issue subpoenas in accord-
2 ance with the civil practice law and rules. The attorney general may
3 also require such other data and information as he or she may deem rele-
4 vant and may require written responses to questions under oath. Such
5 power of subpoena and examination shall not abate or terminate by reason
6 of any action or special proceeding brought by the attorney general
7 under this article.

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

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

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

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

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

32 6. Any consumer who has been injured by a violation of subdivision
33 two, three, eight or nine of section eleven hundred two of this article
34 may bring an action in his or her own name to enjoin such unlawful act
35 or practice and to recover his or her actual damages suffered as a
36 result of the violation. The court may also award reasonable attorneys'
37 fees to a prevailing plaintiff. Actions pursuant to this section may be
38 brought on a class-wide basis.

39 § 1107. Miscellaneous. 1. Preemption: This article does not annul,
40 alter, or affect the laws, ordinances, regulations, or the equivalent
41 adopted by any local entity regarding the processing, collection, trans-
42 fer, disclosure, and sale of consumers' personal data by a controller or
43 processor subject to this article, except to the extent those laws,
44 ordinances, regulations, or the equivalent create requirements or obli-
45 gations that conflict with or reduce the protections afforded to consum-
46 ers under this article.

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

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

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

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

22 § 4. This act shall take effect immediately; provided, however, that
23 sections 1101, 1102, 1103, 1105, 1106 and 1107 of the general business
24 law, as added by section three of this act, shall take effect two years
25 after it shall have become a law but the private right of action author-
26 ized by subdivision 6 of section 1106 of the general business law shall
27 take effect three years after such section shall have become a law.