

STATE OF NEW YORK

680--A

2021-2022 Regular Sessions

IN ASSEMBLY

(Prefiled)

January 6, 2021

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

AN ACT to amend the general business law, in relation to the management
and oversight of personal data

The People of the State of New York, represented in Senate and Assem-
bly, 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 information in ways that can be difficult for ordinary consum-
9 ers to understand. Opaque data processing policies make it impossible to
10 evaluate 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-

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

LBD00516-02-1

1 tronic format, with the ability to transfer it between services; the
2 ability to correct inaccurate data and to delete their data; and the
3 ability to challenge certain automated decisions. This act also imposes
4 obligations upon businesses to maintain reasonable data security for
5 personal data, to notify New York consumers of foreseeable harms arising
6 from use of their data and to obtain specific consent for that use, and
7 to conduct regular assessments to ensure that data is not being used for
8 unacceptable purposes. These data assessments can be obtained and evalu-
9 ated by the New York State Attorney General, who is empowered to obtain
10 penalties for violations of this act and prevent future violations. This
11 act also grants New York consumers who have been injured as the result
12 of a violation a private right of action, which includes reasonable
13 attorneys' fees to a prevailing plaintiff.

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

16 ARTICLE 42

17 NEW YORK PRIVACY ACT

18 Section 1100. Definitions.

19 1101. Jurisdictional scope.

20 1102. Consumer rights.

21 1103. Controller, processor, and third-party responsibilities.

22 1104. Data brokers.

23 1105. Limitations.

24 1106. Enforcement and private right of action.

25 1107. Miscellaneous.

26 § 1100. Definitions. The following definitions apply throughout this
27 article unless the context clearly requires otherwise:

28 1. "Automated decision-making" or "automated decision" means a compu-
29 tational process, including one derived from machine learning, artifi-
30 cial intelligence, or any other automated process, involving personal
31 data that results in a decision affecting a consumer.

32 2. "Biometric information" means any personal data generated from the
33 measurement or specific technological processing of an individual's
34 biological, physical, or physiological characteristics, including fing-
35 erprints, voice prints, iris or retina scans, facial scans or templates,
36 deoxyribonucleic acid (DNA) information, and gait.

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

40 4. "Consent" means a clear affirmative act signifying a freely given,
41 specific, informed, and unambiguous indication of a consumer's agreement
42 to the processing of data relating to the consumer made in response to a
43 dedicated prompt outlining in clear and conspicuous language the materi-
44 al nature of the processing to which the consumer is consenting. A
45 pre-checked box or similar default is not affirmative consent. Consent
46 may be withdrawn at any time, and a controller must provide clear,
47 conspicuous, and consumer-friendly means to withdraw consent. The burden
48 of establishing consent is on the controller.

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

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

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

1 8. "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 controllers or third-parties, the
4 personal data of a consumer with whom it does not have a direct
5 relationship. "Data broker" 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 9. "Deidentified data" means data that cannot reasonably be used to
12 infer information about, or otherwise be linked to a particular consum-
13 er, provided that the processor or controller that possesses the data:

14 (a) takes reasonable measures to ensure that the data cannot be asso-
15 ciated with a consumer or device;

16 (b) publicly commits to process the data only as deidentified data and
17 not attempt to reidentify the data, except that the controller or
18 processor may attempt to reidentify the information solely for the
19 purpose of determining whether its deidentification processes satisfy
20 the requirements of this subdivision; and

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

23 10. "Device" means any physical object that is capable of connecting
24 to the Internet, directly or indirectly, or to another device and is
25 intended for use by a natural person or household or, if used outside
26 the home, for use by the general public.

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

32 12. "Natural person" means a natural person acting only in an individ-
33 ual or household context. It does not include a natural person known to
34 be acting in a commercial or employment context.

35 13. "Person" means a natural person or a legal entity, including but
36 not limited to a proprietorship, partnership, limited partnership,
37 corporation, company, limited liability company or corporation, associ-
38 ation, or other firm or similar body, or any unit, division, agency,
39 department, or similar subdivision thereof.

40 14. "Personal data" means any data that is identified or could reason-
41 ably be linked, directly or indirectly, with a specific natural person,
42 household, or device. Personal data does not include deidentified data.

43 15. "Identified or identifiable natural person" means a natural person
44 who can be identified, directly or indirectly, such as by reference to
45 an identifier such as a name, an identification number, location data,
46 or an online or device identifier.

47 16. "Process," "processes" or "processing" means an operation or set
48 of operations which are performed on data or on sets of data, including
49 but not limited to the collection, use, access, sharing, monetization,
50 analysis, retention, creation, generation, derivation, recording, organ-
51 ization, structuring, storage, disclosure, transmission, analysis,
52 disposal, licensing, destruction, deletion, modification, or deidenti-
53 fication of data.

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

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

19. "Sale," "sell," or "sold" means the disclosure, transfer, conveyance, sharing, licensing, making available, processing, granting of permission or authorization to process, or other exchange of personal data, or providing access to personal data for monetary or other valuable consideration by the controller to a third-party. "Sale" includes enabling, facilitating or providing access to a consumer for targeted advertising. "Sale" does not include the following:

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

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

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

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

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

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

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

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

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

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

2. This article does not apply to:

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

(b) Information that meets the following criteria:

(i) personal data required to be collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley act (P.L. 106-102),

1 and implementing regulations, if the collection, processing, sale, or
2 disclosure is in compliance with such law;

3 (ii) personal data collected, processed, sold, or disclosed pursuant
4 to the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec.
5 2721 et seq.), if the collection, processing, sale, or disclosure is in
6 compliance with that law;

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

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

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

15 (vi) data maintained for employment records purposes, for purposes
16 other than sale;

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

25 (viii) patient identifying information for purposes of 42 C.F.R. Part
26 2, established pursuant to 42 U.S.C. Sec. 290dd-2;

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

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

31 (xi) information originating from, and intermingled to be indistin-
32 guishable from, or information treated in the same manner as, informa-
33 tion exempt under this subdivision that is maintained by a covered enti-
34 ty or business associate as defined by HIPAA or a program or a qualified
35 service organization as defined by 42 U.S.C. § 290dd-2;

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

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

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

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

48 (xiii) patient information maintained by a covered entity or business
49 associate governed by the privacy, security, and breach notification
50 rules issued by the United States Department of Health and Human
51 Services, Parts 160 and 164 of Title 45 of the Code of Federal Regu-
52 lations, established pursuant to the Health Insurance Portability and
53 Accountability Act of 1996 (Public Law 104-191), to the extent the
54 covered entity or business associate maintains the patient information
55 in the same manner as protected health information as described in
56 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;

(c) (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. 1681a(d), and by a user of a consumer report, as set forth in Title 15 U.S.C. Sec. 1681b.; and

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

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

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

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

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

(iv) the purposes for processing personal data;

(v) the identity of each processor or third party to whom the controller discloses, shares, transfers, or sells personal data and, for each identified processor or third party, (A) the categories of personal data being shared, disclosed, transferred, or sold to the processor or third party, (B) the purposes for which personal data is being shared, disclosed, transferred, or sold to the processor or third party, (C) the third party's retention period for each category of personal data processed by the third party or processed on their behalf, or if that is not possible, the criteria used to determine the period, and (D) whether the entity uses the personal data for targeted advertising;

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

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

4 (b) Notice requirements.

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

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

12 (iii) The notice must be dated with its effective date and updated at
13 least annually.

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

17 2. Opt-in consent. (a) A controller must obtain freely given, specif-
18 ic, informed, and unambiguous opt-in consent from a consumer to:

19 (i) process the consumer's personal data for any purpose; or

20 (ii) make any changes in the processing or processing purpose, includ-
21 ing the method and scope of collection, of the consumer's personal data
22 that are less protective of the consumer's personal data than the proc-
23 essing to which the consumer has previously given their freely given,
24 specific, informed, and unambiguous opt-in consent.

25 (b) Any request for consent must, in a standalone disclosure, be
26 provided to the consumer prior to processing their personal data, sepa-
27 rate and apart from any contract or privacy policy. The request for
28 consent must:

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

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

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

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

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

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

53 (c) Targeted advertising and sale of personal data shall not be
54 considered processing purposes that are necessary to provide services or
55 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 personal data for a process-
3 ing 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. The controller may style the mechanism allowing
9 consumers to withdraw previously given consent as an opt-out.

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

14 (g) To the extent that a controller must process internet protocol
15 addresses, system configuration information, URLs of referring pages,
16 locale and language preferences, keystrokes, or any other data that
17 individually or collectively may comprise personal data in order to
18 obtain a consumer's freely given, specific, informed, and unambiguous
19 opt-in consent, the controller must:

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

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

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

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

29 (i) Controllers must treat user-enabled privacy controls in a browser,
30 browser plug-in, smartphone application, operating system, device
31 setting, or other mechanism that communicates or signals the consumer's
32 choice not to be subject to targeted advertising or the sale of their
33 personal data as a denial of consent under this act. To the extent that
34 the privacy control conflicts with a consumer's consent, the privacy
35 control settings govern, unless the consumer provides freely given,
36 specific, informed, and unambiguous opt-in consent to override the
37 privacy control.

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

40 (i) denying services or goods to the consumer, unless the consumer
41 does not consent to processing necessary to provide the services or
42 goods requested by the consumer;

43 (ii) charging different prices for goods or services, including
44 through the use of discounts or other benefits, imposing penalties, or
45 providing a different level or quality of services or goods to the
46 consumer; or

47 (iii) suggesting that the consumer will receive a different price or
48 rate for goods or services or a different level or quality of services
49 or goods.

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

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

6 3. Right to access. Upon the verified request of a consumer, a
7 controller shall:

8 (a) confirm whether or not the controller is processing or has proc-
9 essed personal data of that consumer, and provide access to a copy of
10 any such personal data when requested; and

11 (b) provide the identity of each processor or third-party to whom the
12 controller disclosed, transferred, or sold the consumer's personal data
13 and, for each identified processor or third-party, (A) the categories of
14 the consumer's personal data disclosed, transferred, or sold to each
15 processor or third-party and (B) the purposes for which each category of
16 the consumer's personal data was disclosed, transferred, or sold to each
17 processor or third-party.

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

24 5. Right to correct. (a) Upon the verified request of a consumer, a
25 controller must conduct a reasonable investigation to determine whether
26 personal data, the accuracy of which is disputed by the consumer, is
27 inaccurate, with such investigation to be concluded within the time
28 period set forth in paragraph (a) of subdivision eight of this section.

29 (b) Notwithstanding paragraph (a) of this subdivision, a controller
30 may terminate an investigation of personal data disputed by a consumer
31 under such paragraph if the controller reasonably determines that the
32 dispute by the consumer is frivolous, including by reason of a failure
33 by a consumer to provide sufficient information to investigate the
34 disputed personal data. Upon making any determination in accordance with
35 this paragraph that a dispute is frivolous, a controller must, within
36 the time period set forth in paragraph (a) of subdivision eight of this
37 section, provide the affected consumer a statement in writing that
38 includes, at a minimum, the specific reasons for the determination, and
39 identification of any information required to investigate the disputed
40 personal data, which may consist of a standardized form describing the
41 general nature of such information.

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

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

48 (ii) unless it proves impossible or involves disproportionate effort,
49 communicate such request to each processor or third-party to whom the
50 controller disclosed, transferred, or sold the personal data within one
51 year preceding the consumer's request, and to require those processors
52 or third-parties to do the same for any further processors or third-par-
53 ties they disclosed, transferred, or sold the personal data to.

54 (d) If the investigation does not resolve the dispute, the consumer
55 may file with the controller a brief statement setting forth the nature
56 of the dispute. Whenever a statement of a dispute is filed, unless there

1 exists reasonable grounds to believe that it is frivolous, the control-
2 ler must note that it is disputed by the consumer and include either the
3 consumer's statement or a clear and accurate codification or summary
4 thereof with the disputed personal data whenever it is disclosed, trans-
5 ferred, or sold to any processor or third-party.

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

8 (i) within a reasonable amount of time after receiving the verified
9 request, delete any or all personal data, as directed by the consumer,
10 that the controller possesses or controls; and

11 (ii) unless it proves impossible or involves disproportionate effort,
12 communicate such request to each processor or third-party to whom the
13 controller disclosed, transferred or sold the personal data within one
14 year preceding the consumer's request and to require those processors or
15 third-parties to do the same for any further processors or third-parties
16 they disclosed, transferred, or sold the personal data to.

17 (b) For personal data that is not possessed by the controller but by a
18 processor of the controller, the controller may choose to (i) communi-
19 cate the consumer's request for deletion to the processor, or (ii)
20 request that the processor return to the controller the personal data
21 that is the subject of the consumer's request and delete such personal
22 data upon receipt of the request.

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

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

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

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

38 (ii) it is necessary for the controller to maintain the consumer's
39 personal data to engage in public or peer-reviewed scientific, histor-
40 ical, or statistical research in the public interest that adheres to all
41 other applicable ethics and privacy laws, when the controller's deletion
42 of the information is likely to render impossible or seriously impair
43 the achievement of such research, provided that the consumer has given
44 informed consent and the personal data is not processed for any purpose
45 other than such research.

46 7. Automated decision-making. (a) Whenever a controller makes an auto-
47 mated decision involving solely automated processing that results in a
48 denial of financial or lending services, housing, public accommodation,
49 insurance, health care services, or access to basic necessities, such as
50 food and water, the controller must:

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

53 (ii) provide an avenue for the affected consumer to appeal the deci-
54 sion, which must at minimum allow the affected consumer to (A) express
55 their point of view, (B) contest the decision, and (C) obtain meaningful
56 human review; and

1 (iii) explain how to appeal the decision.

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

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

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

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

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

27 (iii) A controller or processor must make public all impact assess-
28 ments prepared pursuant to this section, retain all such impact assess-
29 ments for at least six years, and make any such retained impact assess-
30 ments available to any state, federal, or local government authority
31 upon request.

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

35 8. Responding to requests. (a) A controller must take action under
36 subdivisions three through six of this section and inform the consumer
37 of any actions taken without undue delay and in any event within forty-
38 five days of receipt of the request. That period may be extended once by
39 forty-five additional days where reasonably necessary, taking into
40 account the complexity and number of the requests. The controller must
41 inform the consumer of any such extension within forty-five days of
42 receipt of the request, together with the reasons for the delay. When a
43 controller denies any such request, it must within this period disclose
44 to the consumer a statement in writing of the specific reasons for the
45 denial.

46 (b) A controller shall permit the exercise of rights and carry out its
47 obligations set forth in subdivisions three through six of this section
48 free of charge, at least twice annually to the consumer. Where requests
49 from a consumer are manifestly unfounded or excessive, in particular
50 because of their repetitive character, the controller may either (i)
51 charge a reasonable fee to cover the administrative costs of complying
52 with the request or (ii) refuse to act on the request and notify the
53 consumer of the reason for refusing the request. The controller bears
54 the burden of demonstrating the manifestly unfounded or excessive char-
55 acter of the request.

1 (c) (i) A controller shall promptly attempt, using commercially
2 reasonable efforts, to verify that all requests to exercise any rights
3 set forth in any section of this article requiring a verified request
4 were made by the consumer who is the subject of the data, or by a person
5 lawfully exercising the right on behalf of the consumer who is the
6 subject of the data. Commercially reasonable efforts shall be determined
7 based on the totality of the circumstances, including the nature of the
8 data implicated by the request.

9 (ii) A controller may require the consumer to provide additional
10 information only if the request cannot reasonably be verified without
11 the provision of such additional information. A controller must not
12 transfer or process any such additional information provided pursuant to
13 this section for any other purpose and must delete any such additional
14 information without undue delay and in any event within forty-five days
15 after the controller has notified the consumer that it has taken action
16 on a request under subdivisions two through five of this section as
17 described in paragraph (a) of this subdivision.

18 (iii) If a controller discloses this additional information to any
19 processor or third-party for the purpose of verifying a consumer
20 request, it must notify the receiving processor or third party at the
21 time of such disclosure, or as close in time to the disclosure as is
22 reasonably practicable, that such information was provided by the
23 consumer for the sole purpose of verification.

24 9. Implementation of rights. Controllers must provide easily accessi-
25 ble and convenient means for consumers to exercise their rights under
26 this article.

27 10. Non-waiver of rights. Any provision of a contract or agreement of
28 any kind that purports to waive or limit in any way a consumer's rights
29 under this article is contrary to public policy and is void and unen-
30 forceable.

31 § 1103. Controller, processor, and third-party responsibilities. 1.
32 Controller responsibilities. (a) Duty of loyalty. (i) Where it is
33 reasonably foreseeable to the controller that a process will be against
34 a consumer's physical, financial, psychological, or reputational inter-
35 ests or against the physical, financial, psychological, or reputational
36 interests of a class of consumers that the consumer is known to belong
37 to, the controller must notify that consumer of any interest that may be
38 harmd in advance of requesting consent and as close in time to the
39 processing as practicable. This obligation does not apply with respect
40 to processing: (A) as required by law; (B) pursuant to a request by a
41 federal, state, or local government or government entity; or (C) that
42 significantly advances protection against criminal or tortious activity.

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

47 (A) designing a user interface with the purpose or substantial effect
48 of deceiving consumers, obscuring consumers' rights under this article,
49 or subverting or impairing user autonomy, decision-making, or choice in
50 order to obtain consent; or

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

53 (b) Duty of care. (i) (A) Controllers must, on at least an annual
54 basis, conduct and document risk assessments of all current processes of
55 personal data.

56 (B) Risk assessments must assess at a minimum:

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

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

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

7 (IV) the adequacy and effect of safeguards implemented by the control-
8 lers;

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

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

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

17 (ii) Controllers must develop, implement, and maintain reasonable
18 safeguards to protect the security, confidentiality and integrity of the
19 personal data of consumers including adopting reasonable administrative,
20 technical and physical safeguards appropriate to the volume and nature
21 of the personal data at issue.

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

27 (B) At least annually, a controller must dispose of all personal data
28 that is either no longer necessary to provide the services or goods
29 requested by the consumer or for the purposes for which the consumer's
30 freely given, specific, informed, and unambiguous opt-in consent is in
31 effect, consistent with the retention period disclosed in notice pursu-
32 ant to section eleven hundred two of this article.

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

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

41 (A) denying services or goods to consumers;

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

45 (C) suggesting that the consumer will receive a different price or
46 rate for services or goods or a different level or quality of services
47 or goods.

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

51 (d) Agreements with processors. (i) Before making any disclosure,
52 transfer, or sale of personal data to any processor, the controller must
53 enter into a written, signed contract with that processor. Such contract
54 must be binding and clearly set forth instructions for processing data,
55 the nature and purpose of processing, the type of data subject to proc-
56 essing, the duration of processing, and the rights and obligations of

1 both parties. The contract must also include requirements that the
2 processor must:

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

5 (B) protect the data consistent with the requirements of this act and
6 any statements made by the controller in their publicly available poli-
7 cies, notices, or similar statements;

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

11 (D) not combine the personal information which the processor receives
12 from or on behalf of the controller with personal information which the
13 processor receives from or on behalf of another person or collects from
14 its own interaction with consumers;

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

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

22 (G) upon the reasonable request of the controller, make available to
23 the controller all information in its possession necessary to demon-
24 strate the processor's compliance with the obligations in this act;

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

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

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

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

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

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

1 (e) Third parties. (i) A controller must not share, disclose, trans-
2 fer, or sell personal data, or facilitate or enable the processing,
3 disclosure, transfer, or sale of personal data to a third party for
4 which consent of the consumer pursuant to subdivision two of section
5 eleven hundred two of this article, has not been obtained or is not
6 currently in effect. Any request for consent to share, disclose, trans-
7 fer, or sell personal data, or to facilitate or enable the processing,
8 disclosure, transfer, or sale of personal data to a third party must
9 clearly include the identity of the third party and the processing
10 purposes for which the third-party may use the personal data.

11 (ii) A controller must not share, disclose, transfer, or sell personal
12 data, or facilitate or enable the processing, disclosure, transfer, or
13 sale of personal data if it can reasonably expect the personal data of a
14 consumer to be used for purposes that the consumer has not consented to
15 pursuant to subdivision two of section eleven hundred two of this arti-
16 cle, or if it can reasonably expect that any rights of the consumer
17 provided in this article would be compromised as a result of such trans-
18 action.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

15 (a) The processing is required by law;

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

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

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

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

24 (i) Register with the attorney general;

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

30 (iii) Provide the following information:

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

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

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

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

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

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

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

49 (b) not sell a consumer's personal data to a data broker that is not
50 registered with the attorney 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, unless the consumer withholds, denies, or with-
47 draws consent; perform a contract to which the consumer is a party; or
48 take steps at the request of the consumer prior to entering into a
49 contract;

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

53 (g) Prevent, detect, protect against, or respond to security inci-
54 dents, identity theft, fraud, harassment, malicious or deceptive activ-
55 ities, or any illegal activity; preserve the integrity or security of

1 systems; or investigate, report, or prosecute those responsible for any
2 such action; or

3 (h) Identify and repair technical errors that impair existing or
4 intended functionality.

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

11 4. The obligations imposed on controllers or processors under this
12 article do not apply to the publication of newsworthy information of
13 legitimate public concern to the public, or the processing or transfer
14 of information by a controller for such purpose.

15 5. A controller that receives a request pursuant to subdivisions three
16 through six of section eleven hundred two of this article, or a process-
17 or or third party to whom a controller communicates such a request, may
18 decline to fulfill the relevant part of such request if:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 1107. Miscellaneous. 1. Preemption: This article does not annul, alter, or affect the laws, ordinances, regulations, or the equivalent adopted by any local entity regarding the processing, collection, transfer, disclosure, and sale of consumers' personal data by a controller or processor subject to this act, except to the extents those laws, ordinances, regulations, or the equivalent are inconsistent with the provisions of this act, and then only to the extent of the inconsistency.

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

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, by an agent authorized by a consumer to exercise the rights set
18 forth in this act on their behalf, or by a parent or guardian authorized
19 by law to take actions of legal consequence on behalf of the consumer
20 who is the subject of the data.

21 § 4. This act shall take effect immediately; provided, however, that
22 sections 1101, 1102, 1103, 1105, 1106 and 1107 of the general business
23 law, as added by section three of this act, shall take effect January 1,
24 2022.