STATE OF NEW YORK

_____

6701--A

2021-2022 Regular Sessions

IN SENATE

May 12, 2021
_____

Introduced by Sens. THOMAS, MAY -- read twice and ordered printed, and
   when printed to be committed to the Committee on Consumer Protection
   -- recommitted to the Committee on Consumer Protection in accordance
   with Senate Rule 6, sec. 8 -- 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 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-

tronic format, with the ability to transfer it between services; the
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 evalu-
ated 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 compu-
tational process, including one derived from machine learning, artifi-
cial 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, including fing-
erprints, 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 estab-
lishing 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.

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

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

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

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

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

9. "Deidentified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to a particular consumer, household or device, provided that the processor or controller that possesses the data:

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

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

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

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

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

12. "Natural person" means a natural person 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.

13. "Person" means a natural person or a legal entity, including but not limited to a proprietorship, partnership, limited partnership, corporation, company, limited liability company or corporation, association, or other firm or similar body, or any unit, division, agency, department, or similar subdivision thereof.

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

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

16. "Process", "processes" or "processing" means an operation or set of operations which are performed on data or on sets of data, including but not limited to the collection, use, access, sharing, monetization, analysis, retention, creation, generation, derivation, recording, organ-

ization, structuring, storage, disclosure, transmission, analysis,
disposal, licensing, destruction, deletion, modification, or deidentifi-
cation of data.
  17. "Processor" means a person that processes data on behalf of the
controller.
  18. "Profiling" means any form of automated processing performed on
personal data to evaluate, analyze, or predict personal aspects related
to an identified or identifiable natural person's economic situation,
health, personal preferences, interests, reliability, behavior,
location, or movements.
  19. "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.
  20. "Sale", "sell", or "sold" means the disclosure, transfer, convey-
ance, 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 valu-
able 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 control-
ler's assets.
  21. "Targeted advertising" means displaying online advertisements to a
consumer where the advertisement is selected based on personal data
obtained or inferred 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 solely on the context of the consum-
er'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.
  22. "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.
  23. "Verified request" means a request by a consumer or their agent 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 more; or

1   (d) derives over fifty percent of gross revenue from the sale of
2   personal data, and controls or processes personal data of twenty-five
3   thousand consumers or more.
4   2. This article does not apply to:
5   (a) personal data processed by state and local governments, and munic-
6   ipal corporations, for processes other than sale (filing and processing
7   fees are not sale);
8   (b) a national securities association registered pursuant to section
9   15A of the Securities Exchange Act of 1934, as amended, or regulations
10 adopted thereunder or a registered futures association so designated
11 pursuant to section 17 of the Commodity Exchange Act, as amended, or any
12 regulations adopted thereunder;
13   (c) information that meets the following criteria:
14   (i) personal data collected, processed, sold, or disclosed pursuant to
15 and in compliance with the federal Gramm-Leach-Bliley act (P.L.
16 106-102), and implementing regulations;
17   (ii) personal data collected, processed, sold, or disclosed pursuant
18 to the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec.
19 2721 et seq.), if the collection, processing, sale, or disclosure is in
20 compliance with that law;
21   (iii) personal data regulated by the federal Family Educational Rights
22 and Privacy Act, U.S.C. Sec. 1232g and its implementing regulations;
23   (iv) personal data collected, processed, sold, or disclosed pursuant
24 to the federal Farm Credit Act of 1971 (as amended in 12 U.S.C. Sec.
25 2001-2279cc) and its implementing regulations (12 C.F.R. Part 600 et
26 seq.) if the collection, processing, sale, or disclosure is in compli-
27 ance with that law;
28   (v) personal data regulated by section two-d of the education law;
29   (vi) data maintained as employment records, for purposes other than
30 sale;
31   (vii) protected health information that is lawfully collected by a
32 covered entity or business associate and is governed by the privacy,
33 security, and breach notification rules issued by the United States
34 Department of Health and Human Services, Parts 160 and 164 of Title 45
35 of the Code of Federal Regulations, established pursuant to the Health
36 Insurance Portability and Accountability Act of 1996 (Public Law
37 104-191) ("HIPAA") and the Health Information Technology for Economic
38 and Clinical Health Act (Public Law 111-5);
39   (viii) patient identifying information for purposes of 42 C.F.R. Part
40 2, established pursuant to 42 U.S.C. Sec. 290dd-2, as long as such data
41 is not sold in violation of HIPAA or any state or federal law;
42   (ix) information and documents lawfully created for purposes of the
43 federal Health Care Quality Improvement Act of 1986, and related regu-
44 lations;
45   (x) patient safety work product created for purposes of 42 C.F.R. Part
46 3, established pursuant to 42 U.S.C. Sec. 299b-21 through 299b-26;
47   (xi) information that is treated in the same manner as information
48 exempt under subparagraph (vii) of this paragraph that is maintained by
49 a covered entity or business associate as defined by HIPAA or a program
50 or a qualified service organization as defined by 42 U.S.C. § 290dd-2,
51 as long as such data is not sold in violation of HIPAA or any state or
52 federal law;
53   (xii) deidentified health information that meets all of the following
54 conditions:

(A) it is deidentified in accordance with the requirements for deiden-
tification 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 reiden-
tify the information nor do they actually reidentify the information
except as otherwise allowed under state or federal law;

(xiii) patient 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 Regu-
lations, 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 patient 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, communi-
cated, disclosed, or sold except as authorized by the Fair Credit
Reporting Act.

§ 1102. Consumer rights. 1. Right to notice. (a) Notice. Each control-
ler 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 third party to whom the controller disclosed, shared, transferred or sold personal data and, for each identified 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) 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 third party 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

(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.

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

(i) process the consumer's personal data for any purpose other than those in subdivision two of section eleven hundred five of this article; or

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

(b) Any request for consent must be provided to the consumer, prior to processing their personal data, in a standalone disclosure that is separate and apart from any contract or privacy policy. The request for consent must:

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

(ii) clearly identify and distinguish between categories of data and
processing purposes that are necessary to provide the services or goods
requested by the consumer and categories of data and processing purposes
that are not necessary to provide the services or goods requested by the
consumer;
(iii) enable a reasonable consumer to easily identify the categories
of data and processing purposes for which consent is sought;
(iv) clearly present as the most conspicuous choice an option to
provide   only   the   consent   necessary to provide the services or goods
requested by the consumer;
(v) clearly present an option to deny consent; and
(vi) where the request seeks consent to sharing, disclosure, transfer,
or sale of personal data to third parties, identify each such third
party, the categories of data sold or shared with them, the processing
purposes, the retention period, or if that is not possible, the criteria
used to determine the period, and for each third party state if such
sharing, disclosure, transfer, or sale enables or involves targeted
advertising. The details of identities of such third parties, and the
categories of data, processing purposes, and the retention period, may
be set forth in a different disclosure, provided that the request for
consent contains a conspicuous and directly accessible link to that
disclosure.
(c) Targeted advertising and sale of personal data shall not be
considered processing purposes that are necessary to provide services or
goods requested by a consumer.
(d) Once a consumer has provided freely given, specific, informed, and
unambiguous opt-in consent to process their personal data for a process-
ing purpose, a controller may rely on such consent until it is with-
drawn.
(e) A controller must provide a mechanism for a consumer to withdraw
previously given consent at any time. Such mechanism shall make it as
easy for a consumer to withdraw their consent as it is for such consumer
to provide consent.
(f) A controller must not infer that a consumer has provided freely
given, specific, informed, and unambiguous opt-in consent from the
consumer's inaction or the consumer's continued use of a service or
product provided by the controller.
(g) To the extent that a controller must process internet protocol
addresses, system configuration information, URLs of referring pages,
locale and language preferences, keystrokes, or any other data that
individually or collectively may comprise personal data in order to
obtain a consumer's freely given, specific, informed, and unambiguous
opt-in consent, the controller must:
(i) process only the personal data necessary to request freely given,
specific, informed, and unambiguous opt-in consent;
(ii) process the personal data solely to request freely given, specif-
ic, informed, and unambiguous opt-in consent; and
(iii) promptly delete the personal data if consent is withheld,
denied, or withdrawn.
(h) Controllers must not request consent from a consumer who has
previously withheld or denied consent, unless consent is necessary to
provide the services or goods requested by the consumer.
(i) Controllers must treat user-enabled privacy controls in a browser,
browser plug-in, smartphone application, operating system, device
setting, or other mechanism that communicates or signals the consumer's
choice not to be subject to targeted advertising or the sale of their

1   personal data as a denial of consent under this act. To the extent that
2   the privacy control conflicts with a consumer's consent, the privacy
3   control settings govern, unless the consumer provides freely given,
4   specific, informed, and unambiguous opt-in consent to override the
5   privacy control.
6   (j) A controller must not discriminate against a consumer for with-
7   holding or denying consent, including, but not limited to, by:
8   (i) denying services or goods to the consumer, unless the consumer
9   does not consent to processing necessary to provide the services or
10 goods requested by the consumer;
11   (ii) charging different prices for goods or services, including
12 through the use of discounts or other benefits, imposing penalties, or
13 providing a different level or quality of services or goods to the
14 consumer; or
15   (iii) suggesting that the consumer will receive a different price or
16 rate for goods or services or a different level or quality of services
17 or goods.
18   (k) A controller may, with the consumer's freely given, specific,
19 informed, and unambiguous opt-in consent given pursuant to this section,
20 operate a program in which information, products, or services sold to
21 the consumer are discounted based solely on such consumer's prior
22 purchases from the controller, provided that the personal data used to
23 operate such program is processed solely for the purpose of operating
24 such program.
25   (l) In the event of a merger, acquisition, bankruptcy, or other trans-
26 action in which another entity assumes control or ownership of all or
27 majority of the controller's assets, any consent provided to the
28 controller by a consumer prior to such transaction shall be deemed with-
29 drawn.
30   3. Right to access. Upon the verified request of a consumer, a
31 controller shall:
32   (a) confirm whether or not the controller is processing or has proc-
33 essed personal data of that consumer, and provide access to a copy of
34 any such personal data in a manner understandable to a reasonable
35 consumer when requested; and
36   (b) provide the identity of each processor or third party to whom the
37 controller disclosed, transferred, or sold the consumer's personal data
38 and, for each identified processor or third party, (i) the categories of
39 the consumer's personal data disclosed, transferred, or sold to each
40 processor or third party and (ii) the purposes for which each category
41 of the consumer's personal data was disclosed, transferred, or sold to
42 each processor or third party.
43   4. Right to portable data. Upon a verified request, and to the extent
44 technically feasible, the controller must: (a) provide to the consumer a
45 copy of all of, or a portion of, as designated in a verified request,
46 the consumer's personal data in a structured, commonly used and
47 machine-readable format and (b) transmit the data to another person of
48 the consumer's or their agent's designation without hindrance.
49   5. Right to correct. (a) Upon the verified request of a consumer or
50 their agent, a controller must conduct a reasonable investigation to
51 determine whether personal data, the accuracy of which is disputed by
52 the consumer, is inaccurate, with such investigation to be concluded
53 within the time period set forth in paragraph (a) of subdivision eight
54 of this section.
55   (b) Notwithstanding paragraph (a) of this subdivision, a controller
56 may terminate an investigation initiated pursuant to such paragraph if

1   the controller reasonably and in good faith determines that the dispute
2   by the consumer is wholly without merit, including by reason of a fail-
3   ure by a consumer to provide sufficient information to investigate the
4   disputed personal data. Upon making any determination in accordance with
5   this paragraph that a dispute is wholly without merit, a controller
6   must, within the time period set forth in paragraph (a) of subdivision
7   eight of this section, provide the affected consumer a statement in
8   writing that includes, at a minimum, the specific reasons for the deter-
9   mination, and identification of any information required to investigate
10 the disputed personal data, which may consist of a standardized form
11 describing the general nature of such information.
12   (c) If, after any investigation under paragraph (a) of this subdivi-
13 sion of any personal data disputed by a consumer, an item of the
14 personal data is found to be inaccurate or incomplete, or cannot be
15 verified, the controller must:
16   (i) correct the inaccurate or incomplete personal data of the consum-
17 er; and
18   (ii) unless it proves impossible or involves disproportionate effort,
19 communicate such request to each processor or third party to whom the
20 controller disclosed, transferred, or sold the personal data within one
21 year preceding the consumer's request, and to require those processors
22 or third parties to do the same for any further processors or third
23 parties they disclosed, transferred, or sold the personal data to.
24   (d) If the investigation does not resolve the dispute, the consumer
25 may file with the controller a brief statement setting forth the nature
26 of the dispute. Whenever a statement of a dispute is filed, unless there
27 exists reasonable grounds to believe that it is wholly without merit,
28 the controller must note that it is disputed by the consumer and include
29 either the consumer's statement or a clear and accurate codification or
30 summary   thereof with the disputed personal data whenever it is
31 disclosed, transferred, or sold to any processor or third party.
32   6. Right to delete. (a) Upon the verified request of a consumer, a
33 controller must:
34   (i) within forty-five days after receiving the verified request,
35 delete any or all personal data, as directed by the consumer or their
36 agent, that the controller possesses or controls; and
37   (ii) unless it proves impossible or involves disproportionate effort
38 that is documented in writing by the controller, communicate such
39 request to each processor or third party to whom the controller
40 disclosed, transferred or sold the personal data within one year preced-
41 ing the consumer's request and to require those processors or third
42 parties to do the same for any further processors or third parties they
43 disclosed, transferred, or sold the personal data to.
44   (b) For personal data that is not possessed by the controller but by a
45 processor of the controller, the controller may choose to (i) communi-
46 cate the consumer's request for deletion to the processor, or (ii)
47 request that the processor return to the controller the personal data
48 that is the subject of the consumer's request and delete such personal
49 data upon receipt of the request.
50   (c) A consumer's deletion of their online account must be treated as a
51 request to the controller to delete all of that consumer's personal
52 data.
53   (d) A controller must maintain reasonable procedures designed to
54 prevent the reappearance in its systems, and in any data it discloses,
55 transfers, or sells to any processor or third party, the personal data
56 that is deleted pursuant to this subdivision.

(e) A controller is not required to comply with a consumer's request
to delete personal data if:
(i) complying with the request would prevent the controller from
performing accounting functions, processing refunds, effectuating a
product recall pursuant to federal or state law, or fulfilling warranty
claims, provided that the personal data that is the subject of the
request is not processed for any purpose other than such specific activ-
ities; or
(ii) it is necessary for the controller to maintain the consumer's
personal data to engage in public or peer-reviewed scientific, histor-
ical, or statistical research in the public interest that adheres to all
other applicable ethics and privacy laws, when the controller's deletion
of the information is likely to render impossible or seriously impair
the achievement of such research, provided that the consumer has given
informed consent and the personal data is not processed for any purpose
other than such research.
7. Automated decision-making. (a) Whenever a controller makes an auto-
mated decision involving solely automated processing that materially
contributes to a denial of financial or lending services, housing,
public accommodation, insurance, health care services, or access to
basic necessities, such as food and water, the controller must:
(i) disclose in a clear, conspicuous, and consumer-friendly manner
that the decision was made by a solely automated process;
(ii) provide an avenue for the affected consumer to appeal the deci-
sion, which must at minimum allow the affected consumer to (A) formally
contest the decision, (B) provide information to support their position,
and (C) obtain meaningful human review of the decision; and
(iii) explain the process to appeal the decision.
(b) A controller must respond to a consumer's appeal within forty-five
days of receipt of the appeal. That period may be extended once by
forty-five additional days where reasonably necessary, taking into
account the complexity and number of appeals. The controller must inform
the consumer of any such extension within forty-five days of receipt of
the appeal, together with the reasons for the delay.
(c) (i) A controller or processor engaged in automated decision-making
affecting financial or lending services, housing, public accommodation,
insurance, education enrollment, employment, health care services, or
access to basic necessities, such as food and water, or engaged in
assisting others in automated decision-making in those fields, must
annually conduct an impact assessment of such automated decision-making
that:
(A) describes and evaluates the objectives and development of the
automated decision-making processes including the design and training
data used to develop the automated decision-making process, how the
automated decision-making process was tested for accuracy, fairness,
bias and discrimination; and
(B) assesses whether the automated decision-making system produces
discriminatory results on the basis of a consumer's or class of consum-
ers' actual or perceived race, color, ethnicity, religion, national
origin, sex, gender, gender identity, sexual orientation, familial
status, biometric information, lawful source of income, or disability.
(ii) A controller or processor must utilize an external, independent
auditor or researcher to conduct such assessments.
(iii) A controller or processor must make publicly available in a
manner accessible online all impact assessments prepared pursuant to
this section, retain all such impact assessments for at least six years,

1 and make any such retained impact assessments available to any state,
2 federal, or local government authority upon request.
3   (iv) For purposes of this paragraph, the limitations to jurisdictional
4 scope set forth in paragraphs (b) and (c) of subdivision two of section
5 eleven hundred one of this article shall not apply.
6   8. Responding to requests. (a) A controller must take action under
7 subdivisions three through six of this section and inform the consumer
8 of any actions taken without undue delay and in any event within forty-
9 five days of receipt of the request. That period may be extended once by
10 forty-five additional days where reasonably necessary, taking into
11 account the complexity and number of the requests. The controller must
12 inform the consumer of any such extension within forty-five days of
13 receipt of the request, together with the reasons for the delay. When a
14 controller denies any such request, it must within this period disclose
15 to the consumer a statement in writing of the specific reasons for the
16 denial.
17   (b) A controller shall permit the exercise of rights and carry out its
18 obligations set forth in subdivisions three through six of this section
19 free of charge, at least twice annually to the consumer. Where requests
20 from a consumer are manifestly unfounded or excessive, in particular
21 because of their repetitive character, the controller may either (i)
22 charge a reasonable fee to cover the administrative costs of complying
23 with the request or (ii) refuse to act on the request and notify the
24 consumer of the reason for refusing the request. The controller bears
25 the burden of demonstrating the manifestly unfounded or excessive char-
26 acter of the request.
27   (c) (i) A controller shall promptly attempt, using commercially
28 reasonable efforts, to verify that all requests to exercise any rights
29 set forth in any section of this article requiring a verified request
30 were made by the consumer who is the subject of the data, or by a person
31 lawfully exercising the right on behalf of the consumer who is the
32 subject of the data. Commercially reasonable efforts shall be determined
33 based on the totality of the circumstances, including the nature of the
34 data implicated by the request.
35   (ii) A controller may require the consumer to provide additional
36 information only if the request cannot reasonably be verified without
37 the provision of such additional information. A controller must not
38 transfer or process any such additional information provided pursuant to
39 this section for any other purpose and must delete any such additional
40 information without undue delay and in any event within forty-five days
41 after the controller has notified the consumer that it has taken action
42 on a request under subdivisions two through five of this section as
43 described in paragraph (a) of this subdivision.
44   (iii) If a controller discloses this additional information to any
45 processor or third party for the purpose of verifying a consumer
46 request, it must notify the receiving processor or third party at the
47 time of such disclosure, or as close in time to the disclosure as is
48 reasonably practicable, that such information was provided by the
49 consumer for the sole purpose of verification and cannot be processed
50 for any purpose other than verification.
51   9. Implementation of rights. Controllers must provide easily accessi-
52 ble and convenient means for consumers to exercise their rights under
53 this article.
54   10. Non-waiver of rights. Any provision of a contract or agreement of
55 any kind that purports to waive or limit in any way a consumer's rights

1 under this article is contrary to public policy and is void and unen-
2 forceable.
3   § 1103. Controller, processor, and third party responsibilities. 1.
4 Controller responsibilities. (a) Data protection assessment. A control-
5 ler shall regularly conduct and document a data protection assessment
6 for processing activities that present a heightened risk of harm to the
7 consumer. Such assessment must identify and weigh the benefits that may
8 flow, directly and indirectly, from the processing to the controller,
9 the consumer, other stakeholders, and the public against the potential
10 risks to the rights of the consumer, or class of consumers, associated
11 with the processing, as mitigated by safeguards that the controller can
12 employ to reduce the risks. The controller shall factor into this
13 assessment the use of deidentified data and the reasonable expectations
14 of consumers, as well as the context of the processing and the relation-
15 ship between the controller and the consumer whose personal data will be
16 processed, with the goal of restricting or prohibiting such processing
17 if the risks of harm to the consumer outweigh the benefits resulting
18 from the processing to the consumer. Processing that presents a height-
19 ened risk of harm to the consumer includes the following:
20   (i) processing that may benefit the controller to the detriment of the
21 consumer;
22   (ii) processing that would be unexpected and highly offensive to a
23 reasonable consumer;
24   (iii) processing personal data for purposes of targeted advertising;
25   (iv) sale of personal data; and
26   (v) processing of personal data for purposes of profiling, where such
27 profiling presents a reasonably foreseeable risk of:
28   (A) unfair or deceptive treatment, or unlawful disparate impact on,
29 consumers or a class of consumers;
30   (B) financial, physical, psychological or reputational injury to
31 consumers, or a class of consumers;
32   (C) a physical or otherwise intrusion upon the solitude or seclusion,
33 or the private affairs or concerns, of consumers, where such intrusion
34 would be offensive to a reasonable person; or
35   (D) other substantial injury to consumers.
36   (b) Duty of loyalty. (i) A controller must notify the consumer, or
37 class of consumers, of the interest that may be harmed in advance of
38 requesting consent and as close in time to the processing as practicable
39 where it is reasonably foreseeable to the controller that a process
40 presents a heightened risk of harm to the consumer or class of consum-
41 ers.
42   (ii) Controllers must not engage in unfair, deceptive, or abusive acts
43 or practices with respect to obtaining consumer consent, the processing
44 of personal data, and a consumer's exercise of any rights under this
45 article, including without limitation:
46   (A) designing a user interface with the purpose or substantial effect
47 of deceiving consumers, obscuring consumers' rights under this article,
48 or subverting or impairing user autonomy, decision-making, or choice in
49 order to obtain consent; or
50   (B) obtaining consent in a manner designed to overpower a consumer's
51 resistance; for example, by making excessive requests for consent.
52   (c) Duty of care. (i) (A) Controllers must, on at least an annual
53 basis, conduct and document risk assessments of all current processing
54 of personal data.
55   (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 control-
lers;

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

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

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

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

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

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

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

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

(A) denying services or goods to consumers;

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

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

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

(e) Agreements with processors. (i) Before making any disclosure,
transfer, or sale of personal data to any processor, the controller must
enter into a written, signed contract with that processor. Such contract

1 **must be binding and clearly set forth instructions for processing data,**
2 **the nature and purpose of processing, the type of data subject to proc-**
3 **essing, the duration of processing, and the rights and obligations of**
4 **both parties. The contract must also include requirements that the**
5 **processor must:**
6 **(A) ensure that each person processing personal data is subject to a**
7 **duty of confidentiality with respect to the data;**
8 **(B) protect the data in a manner consistent with the requirements of**
9 **this act and at least equal to the security requirements of the control-**
10 **ler set forth in their publicly available policies, notices, or similar**
11 **statements;**
12 **(C) process the data only when and to the extent necessary to comply**
13 **with its legal obligations to the controller unless otherwise explicitly**
14 **authorized by the controller;**
15 **(D) not combine the personal data which the processor receives from or**
16 **on behalf of the controller with personal data which the processor**
17 **receives from or on behalf of another person or collects from its own**
18 **interaction with consumers;**
19 **(E) comply with any exercises of a consumer's rights under section**
20 **eleven hundred two of this article upon the request of the controller,**
21 **subject to the limitations set forth in section eleven hundred five of**
22 **this article;**
23 **(F) at the controller's direction, delete or return all personal data**
24 **to the controller as requested at the end of the provision of services,**
25 **unless retention of the personal data is required by law;**
26 **(G) upon the reasonable request of the controller, make available to**
27 **the controller all data in its possession necessary to demonstrate the**
28 **processor's compliance with the obligations in this act;**
29 **(H) allow, and cooperate with, reasonable assessments by the control-**
30 **ler or the controller's designated assessor; alternatively, the process-**
31 **or may arrange for a qualified and independent assessor to conduct an**
32 **assessment of the processor's policies and technical and organizational**
33 **measures in support of the obligations under this article using an**
34 **appropriate and accepted control standard or framework and assessment**
35 **procedure for such assessments. The processor shall provide a report of**
36 **such assessment to the controller upon request;**
37 **(I) a reasonable time in advance before disclosing or transferring the**
38 **data to any further processors, notify the controller of such a proposed**
39 **disclosure or transfer and provide the controller an opportunity to**
40 **approve or reject the proposal; and**
41 **(J) engage any further processor pursuant to a written, signed**
42 **contract that includes the contractual requirements provided in this**
43 **paragraph, containing at minimum the same obligations that the processor**
44 **has entered into with regard to the data.**
45 **(ii) A controller must not agree to indemnify, defend, or hold a**
46 **processor harmless, or agree to a provision that has the effect of**
47 **indemnifying, defending, or holding the processor harmless, from claims**
48 **or liability arising from the processor's breach of the contract**
49 **required by clause (A) of subparagraph (i) of this paragraph or a**
50 **violation of this act. Any provision of an agreement that violates this**
51 **subparagraph is contrary to public policy and is void and unenforceable.**
52 **(iii) Nothing in this paragraph relieves a controller or a processor**
53 **from the liabilities imposed on it by virtue of its role in the process-**
54 **ing relationship as defined by this article.**
55 **(iv) Determining whether a person is acting as a controller or proces-**
56 **sor with respect to a specific processing of data is a fact-based deter-**

1 mination that depends upon the context in which personal data is to be
2 processed. A processor that continues to adhere to a controller's
3 instructions with respect to a specific processing of personal data
4 remains a processor.
5 (f) Third parties. (i) A controller must not share, disclose, trans-
6 fer, or sell personal data, or facilitate or enable the processing,
7 disclosure, transfer, or sale of personal data to a third party for
8 which consent of the consumer pursuant to subdivision two of section
9 eleven hundred two of this article, has not been obtained or is not
10 currently in effect. Any request for consent to share, disclose, trans-
11 fer, or sell personal data, or to facilitate or enable the processing,
12 disclosure, transfer, or sale of personal data to a third party must
13 clearly include the identity of the third party and the processing
14 purposes for which the third party may use the personal data.
15 (ii) A controller must not share, disclose, transfer, or sell personal
16 data, or facilitate or enable the processing, disclosure, transfer, or
17 sale of personal data if it can reasonably expect the personal data of a
18 consumer to be used for purposes that the consumer has not consented to
19 pursuant to subdivision two of section eleven hundred two of this arti-
20 cle, or if it can reasonably expect that any rights of the consumer
21 provided in this article would be compromised as a result of such trans-
22 action.
23 (iii) Before making any disclosure, transfer, or sale of personal data
24 to any third party, the controller must enter into a written, signed
25 contract. Such contract must be binding and the scope, nature, and
26 purpose of processing, the type of data subject to processing, the dura-
27 tion of processing, and the rights and obligations of both parties.
28 Such contract must include requirements that the third party:
29 (A) Process that data only to the extent permitted by the agreement
30 entered into with the controller; and
31 (B) Provide a mechanism to comply with any exercises of a consumer's
32 rights under section eleven hundred two of this article upon the request
33 of the controller, subject to any limitations thereon as authorized by
34 this article; and
35 (C) To the extent the disclosure, transfer, or sale of the personal
36 data causes the third party to become a controller, comply with all
37 obligations imposed on controllers under this article.
38 2. Processor responsibilities. (a) For any personal data that is
39 obtained, received, purchased, or otherwise acquired by a processor,
40 whether directly from a controller or indirectly from another processor,
41 the processor must comply with the requirements set forth in clauses (A)
42 through (J) of subparagraph (i) of paragraph (e) of subdivision one of
43 this section.
44 (b) A processor is not required to comply with a request by the
45 consumer submitted pursuant to this article by a consumer directly to
46 the processor to the extent that the processor has processed the consum-
47 er's personal data solely in its role as a processor for a controller.
48 (c) Processors shall be under a continuing obligation to engage in
49 reasonable measures to review their activities for circumstances that
50 may have altered their ability to identify a specific natural person and
51 to update their classifications of data as identified or identifiable
52 accordingly.
53 (d) A processor shall not engage in any sale of personal data other
54 than on behalf of the controller pursuant to any agreement entered into
55 with the controller.

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

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

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

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

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

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

(a) The processing is required by law;

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

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

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

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

(i) Register with the attorney general;

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

(iii) Provide the following information:

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

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

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

(D) a statement whether the data broker implements a purchaser credentialing process; and

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

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

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

(b) not sell a consumer's personal data to a data broker that is not registered with the attorney general.

 1 3. The attorney general shall establish, manage and maintain a state-
 2 wide registry on its internet website, which shall list all registered
 3 data brokers and make accessible to the public all the information
 4 provided by data brokers pursuant to this section. Printed hard copies
 5 of such registry shall be made available upon request and payment of a
 6 fee to be determined by the attorney general.
 7 4. A data broker that fails to register as required by this section or
 8 submits false information in its registration is, in addition to any
 9 other injunction, penalty, or liability that may be imposed under this
10 article, liable for civil penalties, fees, and costs in an action
11 brought by the attorney general as follows: (a) a civil penalty of one
12 thousand dollars for each day the data broker fails to register as
13 required by this section or fails to correct false information, (b) an
14 amount equal to the fees that were due during the period it failed to
15 register, and (c) expenses incurred by the attorney general in the
16 investigation and prosecution of the action as the court deems appropri-
17 ate.
18 § 1105. Limitations. 1. This article does not require a controller or
19 processor to do any of the following solely for purposes of complying
20 with this article:
21 (a) Reidentify deidentified data;
22 (b) Comply with a verified consumer request to access, correct, or
23 delete personal data pursuant to this article if all of the following
24 are true:
25 (i) The controller is not reasonably capable of associating the
26 request with the personal data;
27 (ii) The controller does not associate the personal data with other
28 personal data about the same specific consumer as part of its normal
29 business practice; and
30 (iii) The controller does not sell the personal data to any third
31 party or otherwise voluntarily disclose or transfer the personal data to
32 any processor or third party, except as otherwise permitted in this
33 article; or
34 (c) Maintain personal data in identifiable form, or collect, obtain,
35 retain, or access any personal data or technology, in order to be capa-
36 ble of associating a verified consumer request with personal data.
37 2. The obligations imposed on controllers and processors under this
38 article do not restrict a controller's or processor's ability to do any
39 of the following, to the extent that the use of the consumer's personal
40 data is reasonably necessary and proportionate for these purposes:
41 (a) Comply with federal, state, or local laws, rules, or regulations;
42 (b) Comply with a civil, criminal, or regulatory inquiry, investi-
43 gation, subpoena, or summons by federal, state, local, or other govern-
44 mental authorities;
45 (c) Cooperate with law enforcement agencies concerning conduct or
46 activity that the controller or processor reasonably and in good faith
47 believes may violate federal, state, or local laws, rules, or regu-
48 lations;
49 (d) Investigate, establish, exercise, prepare for, or defend legal
50 claims;
51 (e) Process personal data necessary to provide the services or goods
52 requested by a consumer; perform a contract to which the consumer is a
53 party; or take steps at the request of the consumer prior to entering
54 into a contract;

(f) Take immediate steps to protect the life or physical safety of the
consumer or of another natural person, and where the processing cannot
be manifestly based on another legal basis;
  (g) Prevent, detect, protect against, or respond to security inci-
dents, identity theft, fraud, harassment, malicious or deceptive activ-
ities, or any illegal activity; preserve the integrity or security of
systems; or investigate, report, or prosecute those responsible for any
such action;
  (h) Identify and repair technical errors that impair existing or
intended functionality; or
  (i) Process business contact information, including a natural person's
name, position name or title, business telephone number, business
address, business electronic mail address, business fax number, or qual-
ifications and any other similar information about the natural person.
  3. The obligations imposed on controllers or processors under this
article do not apply where compliance by the controller or processor
with this article would violate an evidentiary privilege under New York
law and do not prevent a controller or processor from providing personal
data concerning a consumer to a person covered by an evidentiary privi-
lege under New York law as part of a privileged communication.
  4. A controller that receives a request pursuant to subdivisions three
through six of section eleven hundred two of this article, or a process-
or or third party to whom a controller communicates such a request, may
decline to fulfill the relevant part of such request if:
  (a) the controller, processor, or third party is unable to verify the
request using commercially reasonable efforts, as described in paragraph
(c) of subdivision eight of section eleven hundred two of this article;
  (b) complying with the request would be demonstrably impossible (for
purposes of this paragraph, the receipt of a large number of verified
requests, on its own, is not sufficient to render compliance with a
request demonstrably impossible);
  (c) complying with the request would impair the privacy of another
individual or the rights of another to exercise free speech; or
  (d) the personal data was created by a natural person other than the
consumer making the request and is being processed for the purpose of
facilitating interpersonal relationships or public discussion.
  § 1106. Enforcement and private right of action. 1. Whenever it
appears to the attorney general, either upon complaint or otherwise,
that any person or persons has engaged in or is about to engage in any
of the acts or practices stated to be unlawful under this article, the
attorney general may bring an action or special proceeding in the name
and on behalf of the people of the state of New York to enjoin any
violation of this article, to obtain restitution of any moneys or prop-
erty obtained directly or indirectly by any such violation, to obtain
disgorgement of any profits obtained directly or indirectly by any such
violation, to obtain civil penalties of not more than fifteen thousand
dollars per violation, and to obtain any such other and further relief
as the court may deem proper, including preliminary relief.
  (a) Any action or special proceeding brought by the attorney general
pursuant to this section must be commenced within six years.
  (b) Each instance of unlawful processing counts as a separate
violation. Unlawful processing of the personal data of more than one
consumer counts as a separate violation as to each consumer. Each
provision of this article that is violated counts as a separate
violation.

 1 (c) In assessing the amount of penalties, the court must consider any
 2 one or more of the relevant circumstances presented by any of the
 3 parties, including, but not limited to, the nature and seriousness of
 4 the misconduct, the number of violations, the persistence of the miscon-
 5 duct, the length of time over which the misconduct occurred, the will-
 6 fulness of the violator's misconduct, and the violator's financial
 7 condition.
 8 2. In connection with any proposed action or special proceeding under
 9 this section, the attorney general is authorized to take proof and make
10 a determination of the relevant facts, and to issue subpoenas in accord-
11 ance with the civil practice law and rules. The attorney general may
12 also require such other data and information as he or she may deem rele-
13 vant and may require written responses to questions under oath.   Such
14 power of subpoena and examination shall not abate or terminate by reason
15 of any action or special proceeding brought by the attorney general
16 under this article.
17 3. Any person, within or outside the state, who the attorney general
18 believes may be in possession, custody, or control of any books, papers,
19 or other things, or may have information, relevant to acts or practices
20 stated to be unlawful in this article is subject to the service of a
21 subpoena issued by the attorney general pursuant to this section.
22 Service may be made in any manner that is authorized for service of a
23 subpoena or a summons by the state in which service is made.
24 4. (a) Failure to   comply with a subpoena issued pursuant to this
25 section without reasonable cause tolls the applicable statutes of limi-
26 tations in any action or special proceeding brought by the attorney
27 general against the noncompliant person that arises out of the attorney
28 general's investigation.
29 (b) If a person fails to comply with a subpoena issued pursuant to
30 this section, the attorney general may move in the supreme court to
31 compel compliance. If the court finds that the subpoena was authorized,
32 it shall order compliance and may impose a civil penalty of up to five
33 hundred dollars per day of noncompliance.
34 (c) Such tolling and civil penalty shall be in addition to any other
35 penalties or remedies provided by law for noncompliance with a subpoena.
36 5. This section shall apply to all acts declared to be unlawful under
37 this article, whether or not subject to any other law of this state, and
38 shall not supersede, amend or repeal any other law of this state under
39 which the attorney general is authorized to take any action or conduct
40 any inquiry.
41 6. Any consumer who has been injured by a violation of subdivision
42 two, seven or eight of section eleven hundred two of this article may
43 bring an action in his or her own name to enjoin such unlawful act or
44 practice and to recover his or her actual damages or one thousand
45 dollars, whichever is greater. The court may also award reasonable
46 attorneys' fees to a prevailing plaintiff. Actions pursuant to this
47 section may be brought on a class-wide basis.
48 § 1107. Miscellaneous. 1. Preemption: This article does not annul,
49 alter, or affect the laws, ordinances, regulations, or the equivalent
50 adopted by any local entity regarding the processing, collection, trans-
51 fer, disclosure, and sale of consumers' personal data by a controller or
52 processor subject to this article, except to the extent those laws,
53 ordinances, regulations, or the equivalent create requirements or obli-
54 gations that conflict with or reduce the protections afforded to consum-
55 ers under this article.

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 commit- tees of the legislature within two years of the effective date of this section.

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

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

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

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