STATE OF NEW YORK

365--A

2023-2024 Regular Sessions

IN SENATE

(Prefiled)

January 4, 2023

_____

Introduced by Sens. THOMAS, COMRIE, JACKSON, KRUEGER, MAY, RAMOS -- read
  twice and ordered printed, and when printed to be committed to the
  Committee on Consumer Protection -- reported favorably from said
  committee and committed to the Committee on Internet and Technology --
  committee discharged, bill amended, ordered reprinted as amended and
  recommitted to said committee

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

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

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

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

notice of how their data is being used, processed and shared; the abili-
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.
  § 3. The general business law is amended by adding a new article 42 to
read as follows:

<div align="center">

ARTICLE 42

NEW YORK PRIVACY ACT

</div>

Section 1100. Definitions.
**   1101. Jurisdictional scope.**
**   1102. Consumer rights.**
**   1103. Controller, processor, and third party responsibilities.**
**   1104. Data brokers.**
**   1105. Limitations.**
**   1106. Enforcement.**
**   1107. Miscellaneous.**
** § 1100. Definitions. The following definitions apply for the purposes**
of this article unless the context clearly requires otherwise:
** 1. "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 that allows or
confirms the unique identification of a natural person, including fing-
erprints, voice prints, iris or retina scans, facial scans or templates,
deoxyribonucleic acid (DNA) information, and gait. "Biometric informa-
tion" does not include a digital or physical photograph, an audio or
video recording, or any data generated from a digital or physical photo-
graph, or an audio or video recording, unless such data is generated to
identify a specific individual.
** 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.

1   5. "Consumer" means a natural person who is a New York resident acting
2   only in an individual or household context. It does not include a
3   natural person known to be acting in a professional or employment
4   context.
5   6. "Controller" means the person who, alone or jointly with others,
6   determines the purposes and means of the processing of personal data.
7   7. "Covered entity" has the same meaning as in Title 45 of the C.F.R.,
8   established pursuant to the federal Health Insurance Portability and
9   Accountability Act of 1996.
10   8. "Data broker" means a person, or unit or units of a legal entity,
11   separately or together, that does business in the state of New York and
12   knowingly collects, and sells to other controllers or third parties, the
13   personal data of a consumer with whom it does not have a direct
14   relationship. "Data broker" does not include any of the following:
15   (a) a consumer reporting agency to the extent that it is covered by
16   the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.); or
17   (b) a financial institution to the extent that it is covered by the
18   Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regu-
19   lations.
20   9. "Decisions that produce legal or similarly significant effects"
21   means decisions made by the controller that result in the provision or
22   denial by the controller of financial or lending services, housing,
23   insurance, education enrollment or opportunity, criminal justice,
24   employment opportunities, health care services or access to essential
25   goods or services.
26   10. "Deidentified data" means data that cannot reasonably be used to
27   infer information about, or otherwise be linked to a particular consum-
28   er, household or device, provided that the processor or controller that
29   possesses the data:
30   (a) implements reasonable technical safeguards to ensure that the data
31   cannot be associated with a consumer, household or device;
32   (b) publicly commits to process the data only as deidentified data and
33   not attempt to reidentify the data, except that the controller or
34   processor may attempt to reidentify the information solely for the
35   purpose of determining whether its deidentification processes satisfy
36   the requirements of this subdivision; and
37   (c) contractually obligates any recipients of the data to comply with
38   all provisions of this article.
39   11. "Device" means any physical object that is capable of connecting
40   to the internet, directly or indirectly, or to another device and is
41   intended for use by a natural person or household or, if used outside
42   the home, for use by the general public.
43   12. "Household" means a group, however identified, of consumers who
44   cohabitate with one another at the same residential address and may
45   share use of common devices or services.
46   13. "Identified or identifiable" means a natural person who can be
47   identified, directly or indirectly, such as by reference to an identifi-
48   er such as a name, an identification number, location data, or an online
49   or device identifier.
50   14. "Meaningful human review" means review or oversight by one or more
51   individuals who (a) are trained in the capabilities and limitations of
52   the algorithm at issue and the procedures to interpret and act on the
53   output of the algorithm, and (b) have the authority to alter the auto-
54   mated decision under review.

1   15. "Natural person" means a natural person acting only in an individ-
2   ual or household context. It does not include a natural person known to
3   be acting in a professional or employment context.
4   16. "Person" means a natural person or a legal entity, including but
5   not limited to a proprietorship, partnership, limited partnership,
6   corporation, company, limited liability company or corporation, associ-
7   ation, or other firm or similar body, or any unit, division, agency,
8   department, or similar subdivision thereof.
9   17. "Personal data" means any data that identifies or could reasonably
10 be linked, directly or indirectly, with a specific natural person, or
11 household. Personal data does not include deidentified data, informa-
12 tion that is lawfully made publicly available from federal, state or
13 local government records, or information that a controller has a reason-
14 able basis to believe is lawfully made available to the general public
15 by the consumer or from widely distributed media.
16 18. "Precise geolocation data" means information derived from technol-
17 ogy, including, but not limited to, global position system level lati-
18 tude and longitude coordinates or other mechanisms, that directly iden-
19 tifies the specific location of an individual with precision and
20 accuracy within a radius of one thousand seven hundred fifty feet,
21 except as prescribed by regulations. Precise geolocation data does not
22 include the content of communications or any data generated by or
23 connected to advance utility metering infrastructure systems or equip-
24 ment for use by a utility.
25 19. "Process", "processes" or "processing" means an operation or set
26 of operations which are performed on data or on sets of data, including
27 but not limited to the collection, use, access, sharing, monetization,
28 analysis, retention, creation, generation, derivation, recording, organ-
29 ization, structuring, storage, disclosure, transmission, analysis,
30 disposal, licensing, destruction, deletion, modification, or deidentifi-
31 cation of data.
32 20. "Processor" means a person that processes data on behalf of the
33 controller.
34 21. "Profiling" means any form of automated processing performed on
35 personal data to evaluate, analyze, or predict personal aspects related
36 to an identified or identifiable natural person's economic situation,
37 health, personal preferences, interests, reliability, behavior,
38 location, or movements. Profiling does not include evaluation, analy-
39 sis, or prediction based solely upon a natural person's current search
40 query or activities on, or current visit to, the controller's website or
41 online application.
42 22. "Protected health information" has the same meaning as in Title 45
43 C.F.R., established pursuant to the federal Health Insurance Portability
44 and Accountability Act of 1996.
45 23. "Sale", "sell", or "sold" means the disclosure, transfer, convey-
46 ance, sharing, licensing, making available, processing, granting of
47 permission or authorization to process, or other exchange of personal
48 data, or providing access to personal data for monetary or other valu-
49 able consideration by the controller to a third party. "Sale" includes
50 enabling, facilitating or providing access to personal data for targeted
51 advertising. "Sale" does not include the following:
52 (a) the disclosure of data to a processor who processes the data on
53 behalf of the controller and which is contractually prohibited from
54 using it for any purpose other than as instructed by the controller;
55 (b) the disclosure or transfer of data as an asset that is part of a
56 merger, acquisition, bankruptcy, or other transaction in which another

1 entity assumes control or ownership of all or a majority of the control-
2 ler's assets; or
3   (c) the disclosure of presonal data to a third party necessary for
4 purposes of providing a product, service, or interaction with such third
5 party, when the consumer intentionally and unambiguously requests such
6 disclosure.
7   24. "Sensitive data" means personal data that reveals:
8   (a) racial or ethnic origin, religious beliefs, mental or physical
9 health condition or diagnosis, sex life, sexual orientation, or citizen-
10 ship or immigration status;
11   (b) genetic or biometric information for the purpose of uniquely iden-
12 tifying a natural person;
13   (c) precise geolocation data; or
14   (d) social security, financial account, passport or driver's license
15 numbers.
16   25. "Targeted advertising" means advertising based upon profiling.
17   26. "Third party" means, with respect to a particular interaction or
18 occurrence, a person, public authority, agency, or body other than the
19 consumer, the controller, or processor of the controller. A third party
20 may also be a controller if the third party, alone or jointly with
21 others, determines the purposes and means of the processing of personal
22 data.
23   27. "Verified request" means a request by a consumer or their agent to
24 exercise a right authorized by this article, the authenticity of which
25 has been ascertained by the controller in accordance with paragraph (c)
26 of subdivision eight of section eleven hundred two of this article.
27   § 1101. Jurisdictional scope. 1. This article applies to legal persons
28 that conduct business in New York or produce products or services that
29 are targeted to residents of New York, and that satisfy one or more of
30 the following thresholds:
31   (a) have annual gross revenue of twenty-five million dollars or more;
32   (b) controls or processes personal data of fifty thousand consumers or
33 more; or
34   (c) derives over fifty percent of gross revenue from the sale of
35 personal data.
36   2. This article does not apply to:
37   (a) personal data processed by state and local governments, and munic-
38 ipal corporations, for processes other than sale (filing and processing
39 fees are not sale);
40   (b) a national securities association registered pursuant to section
41 15A of the Securities Exchange Act of 1934, as amended, or regulations
42 adopted thereunder or a registered futures association so designated
43 pursuant to section 17 of the Commodity Exchange Act, as amended, or any
44 regulations adopted thereunder;
45   (c) any nonprofit entity identified in section four hundred five of
46 the financial services law to the extent such organization collects,
47 processes, uses, or shares data solely in relation to identifying,
48 investigating, or assisting (i) law enforcement agencies in connection
49 with suspected insurance-related criminal or fraudulent acts; or (ii)
50 first responders in connection with catastrophic events;
51   (d) information that meets the following criteria:
52   (i) personal data collected, processed, sold, or disclosed pursuant to
53 and in compliance with the federal Gramm-Leach-Bliley act (P.L.
54 106-102), and implementing regulations;
55   (ii) personal data collected, processed, sold, or disclosed pursuant
56 to the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec.

2721 et seq.), if the collection, processing, sale, or disclosure is in
compliance with that law;
   (iii) personal data regulated by the federal Family Educational Rights
and Privacy Act, U.S.C. Sec. 1232g and its implementing regulations;
   (iv) personal data collected, processed, sold, or disclosed pursuant
to the federal Farm Credit Act of 1971 (as amended in 12 U.S.C. Sec.
2001-2279cc) and its implementing regulations (12 C.F.R. Part 600 et
seq.) if the collection, processing, sale, or disclosure is in compli-
ance with that law;
   (v) personal data regulated by section two-d of the education law;
   (vi) data maintained as employment records, for purposes other than
sale;
   (vii) protected health information that is lawfully collected by a
covered entity or business associate and is governed by the privacy,
security, and breach notification rules issued by the United States
Department of Health and Human Services, Parts 160 and 164 of Title 45
of the Code of Federal Regulations, established pursuant to the Health
Insurance Portability and Accountability Act of 1996 (Public Law
104-191) ("HIPAA") and the Health Information Technology for Economic
and Clinical Health Act (Public Law 111-5);
   (viii) patient identifying information for purposes of 42 C.F.R. Part
2, established pursuant to 42 U.S.C. Sec. 290dd-2, as long as such data
is not sold in violation of HIPAA or any state or federal law;
   (ix) information and documents lawfully created for purposes of the
federal Health Care Quality Improvement Act of 1986, and related regu-
lations;
   (x) patient safety work product created for purposes of 42 C.F.R. Part
3, established pursuant to 42 U.S.C. Sec. 299b-21 through 299b-26;
   (xi) information that is treated in the same manner as information
exempt under subparagraph (vii) of this paragraph that is maintained by
a covered entity or business associate as defined by HIPAA or a program
or a qualified service organization as defined by 42 U.S.C. § 290dd-2,
as long as such data is not sold in violation of HIPAA or any state or
federal law;
   (xii) deidentified health information that meets all of the following
conditions:
   (A) it is deidentified in accordance with the requirements for 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) information maintained by a covered entity or business associ-
ate governed by the privacy, security, and breach notification rules
issued by the United States Department of Health and Human Services,
Parts 160 and 164 of Title 45 of the Code of Federal Regulations, estab-
lished pursuant to the Health Insurance Portability and Accountability
Act of 1996 (Public Law 104-191), to the extent the covered entity or
business associate maintains the information in the same manner as
protected health information as described in subparagraph (vii) of this
paragraph;

1 (xiv) data collected as part of human subjects research, including a
2 clinical trial, conducted in accordance with the Federal Policy for the
3 Protection of Human Subjects, also known as the Common Rule, pursuant to
4 good clinical practice guidelines issued by the International Council
5 for Harmonisation or pursuant to human subject protection requirements
6 of the United States Food and Drug Administration;
7 (xv) personal data processed only for one or more of the following
8 purposes:
9 (A) product registration and tracking consistent with applicable
10 United States Food and Drug Administration regulations and guidance;
11 (B) public health activities and purposes as described in Section
12 164.512 of Title 45 of the Code of Federal Regulations; and/or
13 (C) activities related to quality, safety, or effectiveness regulated
14 by the United States Food and Drug Administration; or
15 (xvi) personal data collected, processed, or disclosed pursuant to and
16 in compliance with any opt-out program authorized by the public service
17 commission or any other opt-out community distributed generation
18 programs authorized in law; or
19 (e) (i) an activity involving the collection, maintenance, disclosure,
20 sale, communication, or use of any personal data bearing on a consumer's
21 credit worthiness, credit standing, credit capacity, character, general
22 reputation, personal characteristics, or mode of living by a consumer
23 reporting agency, as defined in Title 15 U.S.C. Sec. 1681a(f), by a
24 furnisher of information, as set forth in Title 15 U.S.C. Sec. 1681s-2,
25 who provides information for use in a consumer report, as defined in
26 Title 15 U.S.C. Sec. 1861a(d), and by a user of a consumer report, as
27 set forth in Title 15 U.S.C. Sec. 1681b.; and
28 (ii) this paragraph shall apply only to the extent that such activity
29 involving the collection, maintenance, disclosure, sale, communication,
30 or use of such data by that agency, furnisher, or user is subject to
31 regulation under the Fair Credit Reporting Act, Title 15 U.S.C. Sec.
32 1681 et seq., and the data is not collected, maintained, used, communi-
33 cated, disclosed, or sold except as authorized by the Fair Credit
34 Reporting Act.
35 § 1102. Consumer rights. 1. Right to notice. (a) Notice. Each control-
36 ler that processes a consumer's personal data must make publicly and
37 consistently available, in a conspicuous and readily accessible manner,
38 a notice containing the following:
39 (i) a description of the consumer's rights under subdivisions two
40 through seven of this section and how a consumer may exercise those
41 rights, including how to withdraw consent;
42 (ii) the categories of personal data processed by the controller and
43 by any processor who processes personal data on behalf of the control-
44 ler;
45 (iii) the sources from which personal data is collected;
46 (iv) the purposes for processing personal data;
47 (v) the categories of third parties to whom the controller disclosed,
48 shared, transferred or sold personal data and, for each category of
49 third party, (A) the categories of personal data being shared,
50 disclosed, transferred, or sold to the third party, (B) the purposes for
51 which personal data is being shared, disclosed, transferred, or sold to
52 the third party, (C) any applicable retention periods for each category
53 of personal data processed by the third parties or processed on their
54 behalf, or if that is not possible, the criteria used to determine the
55 period, and (D) whether the third parties may use the personal data for
56 targeted advertising; and

1   (vi) the controller's retention period for each category of personal
2   data that they process or is processed on their behalf, or if that is
3   not possible, the criteria used to determine that period.
4   (b) Notice requirements.
5   (i) The notice must be written in easy-to-understand language and
6   format at an eighth grade reading level or below and in at least twelve
7   point font.
8   (ii) The categories of personal data processed and purposes for which
9   each category of personal data is processed must be described in a clear
10 and conspicuous manner, at a level specific enough to enable a consumer
11 to exercise meaningful control over their personal data but not so
12 specific as to render the notice unhelpful to a consumer.
13   (iii) The notice must be dated with its effective date and updated at
14 least annually. When the information required to be disclosed to a
15 consumer pursuant to paragraph (a) of this subdivision has not changed
16 since the immediately previous notice (whether initial, annual, or
17 revised) provided to the consumer, a controller may issue a statement
18 that no changes have been made.
19   (iv) The notice, as well as each version of the notice in effect in
20 the preceding six years, must be easily accessible to consumers and
21 capable of being viewed by consumers at any time.
22   2. Right to opt out. (a) A controller must allow consumers the right
23 to opt out, at any time, of processing personal data concerning the
24 consumer for the purposes of:
25   (i) targeted advertising;
26   (ii) the sale of personal data; and
27   (iii) profiling in furtherance of decisions that produce legal or
28 similarly significant effects concerning a consumer.
29   (b) A controller must provide clear and conspicuous means for the
30 consumer or their agent to opt out of processing and clearly present as
31 the most conspicuous choice an option to simultaneously opt out of all
32 processing purposes set forth in paragraph (a) of this subdivision.
33   (c) A controller must not process personal data for any purpose from
34 which the consumer has opted out.
35   (d) A controller must not request that a consumer who has opted out of
36 certain purposes of processing personal data opt back in, unless those
37 purposes subsequently become necessary to provide the services or goods
38 requested by a consumer. Targeted advertising and sale of personal data
39 shall not be considered processing purposes that are necessary to
40 provide service or goods requested by a consumer.
41   (e) Controllers must treat user-enabled privacy controls in a browser,
42 browser plug-in, smartphone application, operating system, device
43 setting, or other mechanism that communicates or signals the consumer's
44 choice not to opt out of the processing of personal data in furtherance
45 of targeted advertising, the sale of their personal data, or profiling
46 in furtherance of decisions that produce legal or similarly significant
47 effects concerning the consumer as an opt out under this article. To the
48 extent that the privacy control conflicts with a consumer's consent, the
49 controller shall comply with the privacy control but may notify the
50 consumer of such conflict and provide to such consumer the choice to
51 give controller specific consent to such processing.
52   3. Sensitive data. (a) A controller must obtain freely given, specif-
53 ic, informed, and unambiguous opt-in consent from a consumer to:
54   (i) process the consumer's sensitive data related to that consumer for
55 any purpose other than those in subdivision two of section eleven
56 hundred five of this article; or

1 (ii) make any changes to the existing processing or processing
2 purpose, including those regarding the method and scope of collection,
3 of the consumer's sensitive data that may be less protective of the
4 consumer's sensitive data than the processing to which the consumer has
5 previously given their freely given, specific, informed, and unambiguous
6 opt-in consent.
7 (b) Any request for consent to process sensitive data must be provided
8 to the consumer, prior to processing their sensitive data, in a stand-
9 alone disclosure that is separate and apart from any contract or privacy
10 policy. The request for consent must:
11 (i) be written in a twelve point font or greater and include a clear
12 and conspicuous description of each category of data and processing
13 purpose for which consent is sought;
14 (ii) clearly identify and distinguish between categories of data and
15 processing purposes that are necessary to provide the services or goods
16 requested by the consumer and categories of data and processing purposes
17 that are not necessary to provide the services or goods requested by the
18 consumer;
19 (iii) enable a reasonable consumer to easily identify the categories
20 of data and processing purposes for which consent is sought;
21 (iv) clearly present as the most conspicuous choice an option to
22 provide only the consent necessary to provide the services or goods
23 requested by the consumer;
24 (v) clearly present an option to deny consent; and
25 (vi) where the request seeks consent to sharing, disclosure, transfer,
26 or sale of sensitive data to third parties, identify the categories of
27 such third parties, the categories of data sold or shared with them, the
28 processing purposes, the retention period, or if that is not possible,
29 the criteria used to determine the period, and state if such sharing,
30 disclosure, transfer, or sale enables or involves targeted advertising.
31 The details of the categories of such third parties, and the categories
32 of data, processing purposes, and the retention period, may be set forth
33 in a different disclosure, provided that the request for consent
34 contains a conspicuous and directly accessible link to that disclosure.
35 (c) Targeted advertising and sale of personal data shall not be
36 considered processing purposes that are necessary to provide services or
37 goods requested by a consumer.
38 (d) Once a consumer has provided freely given, specific, informed, and
39 unambiguous opt-in consent to process their sensitive data for a proc-
40 essing purpose, a controller may rely on such consent until it is with-
41 drawn.
42 (e) A controller must provide a mechanism for a consumer to withdraw
43 previously given consent at any time. Such mechanism shall make it as
44 easy for a consumer to withdraw their consent as it is for such consumer
45 to provide consent.
46 (f) A controller must not infer that a consumer has provided freely
47 given, specific, informed, and unambiguous opt-in consent from the
48 consumer's inaction or the consumer's continued use of a service or
49 product provided by the controller.
50 (g) Controllers must not request consent from a consumer who has
51 previously withheld or denied consent to process sensitive data, until
52 at least twelve months after a denial, unless consent is necessary to
53 provide the services or goods requested by the consumer.
54 (h) Controllers must treat user-enabled privacy controllers in a brow-
55 ser, browser plug-in, smartphone application, operating system, device
56 setting, or other mechanism that communicates or signals the consumer's

1 choices to opt out of the processing of personal data in furtherance of
2 targeted advertising, the sale of their personal data, or profiling in
3 furtherance of decisions that produce legal or similarly significant
4 effects concerning the consumer as a denial of consent to process sensi-
5 tive data under this article. To the extent that the privacy control
6 conflicts with a consumer's consent, the privacy control settings
7 govern, unless the consumer provides freely given, specific, informed,
8 and unambiguous opt-in consent to override the privacy control, however,
9 the controller may notify such consumer of such conflict and provide to
10 the   consumer the choice to give controller-specific consent to such
11 processing.
12   (i) (i) A controller must not discriminate against a consumer for
13 withholding or denying consent, including, but not limited to, by:
14   (A) denying services or goods to the consumer, unless the consumer
15 does not consent to processing necessary to provide the services or
16 goods requested by the consumer;
17   (B) charging different prices for goods or services, including through
18 the use of discounts or other benefits, imposing penalties, or providing
19 a different level or quality of services or goods to the consumer; or
20   (C) suggesting that the consumer will receive a different price or
21 rate for goods or services or a different level or quality of services
22 or goods.
23   (ii) A controller shall not be prohibited from offering a different
24 price, rate, level, quality, or selection of goods or services to a
25 consumer, including offering goods or services for no fee, if the offer-
26 ing is in connection with a consumer's voluntary participation in bona
27 fide loyalty, rewards, premium features, discounts, or club card
28 program. If a consumer exercises their right pursuant to paragraph (a)
29 of subdivision two of this section, a controller may not sell personal
30 data to a third party controller as part of such a program unless: (A)
31 the sale is reasonably necessary to enable the third party to provide a
32 benefit to which the consumer is entitled; (B) the sale of personal data
33 to third parties is clearly disclosed in the terms of the program; and
34 (C) the third party uses the personal data only for purposes of facili-
35 tating such a benefit to which the consumer is entitled and does not
36 retain or otherwise use or disclose the personal data for any other
37 purpose.
38   (j) A controller may, with the consumer's freely given, specific,
39 informed, and unambiguous opt-in consent given pursuant to this section,
40 operate a program in which information, products, or services sold to
41 the consumer are discounted based solely on such consumer's prior
42 purchases from the controller, provided that any sensitive data used to
43 operate such program is processed solely for the purpose of operating
44 such program.
45   (k) In the event of a merger, acquisition, bankruptcy, or other trans-
46 action in which another entity assumes control or ownership of all or
47 majority of the controller's assets, any consent provided to the
48 controller by a consumer relating to sensitive data prior to such trans-
49 action other than consent to processing necessary to provide services or
50 goods requested by the consumer, shall be deemed withdrawn.
51   4. Right to access. Upon the verified request of a consumer, a
52 controller shall:
53   (a) confirm whether or not the controller is processing or has proc-
54 essed personal data of that consumer, and provide access to a copy of
55 any such personal data in a manner understandable to a reasonable
56 consumer when requested; and

1   (b) provide the category of each processor or third party to whom the
2 controller disclosed, transferred, or sold the consumer's personal data
3 and, for each category of processor or third party, (i) the categories
4 of the consumer's personal data disclosed, transferred, or sold to each
5 processor or third party and (ii) the purposes for which each category
6 of the consumer's personal data was disclosed, transferred, or sold to
7 each processor or third party.
8   5. Right to portable data. Upon a verified request, and to the extent
9 technically feasible, the controller must: (a) provide to the consumer a
10 copy of all of, or a portion of, as designated in a verified request,
11 the consumer's personal data in a structured, commonly used and
12 machine-readable format and (b) transmit the data to another person of
13 the consumer's or their agent's designation without hindrance.
14   6. Right to correct. (a) Upon the verified request of a consumer or
15 their agent, a controller must conduct a reasonable investigation to
16 determine whether personal data, the accuracy of which is disputed by
17 the consumer, is inaccurate, with such investigation to be concluded
18 within the time period set forth in paragraph (a) of subdivision eight
19 of this section.
20   (b) Notwithstanding paragraph (a) of this subdivision, a controller
21 may terminate an investigation initiated pursuant to such paragraph if
22 the controller reasonably and in good faith determines that the dispute
23 by the consumer is wholly without merit, including by reason of a fail-
24 ure by a consumer to provide sufficient information to investigate the
25 disputed personal data. Upon making any determination in accordance with
26 this paragraph that a dispute is wholly without merit, a controller
27 must, within the time period set forth in paragraph (a) of subdivision
28 eight of this section, provide the affected consumer a statement in
29 writing that includes, at a minimum, the specific reasons for the deter-
30 mination, and identification of any information required to investigate
31 the disputed personal data, which may consist of a standardized form
32 describing the general nature of such information.
33   (c) If, after any investigation under paragraph (a) of this subdivi-
34 sion of any personal data disputed by a consumer, an item of the
35 personal data is found to be inaccurate or incomplete, or cannot be
36 verified, the controller must:
37   (i) correct the inaccurate or incomplete personal data of the consum-
38 er; and
39   (ii) unless it proves impossible or involves disproportionate effort,
40 communicate such request to each processor or third party to whom the
41 controller disclosed, transferred, or sold the personal data within one
42 year preceding the consumer's request, and to require those processors
43 or third parties to do the same for any further processors or third
44 parties they disclosed, transferred, or sold the personal data to.
45   (d) If the investigation does not resolve the dispute, the consumer
46 may file with the controller a brief statement setting forth the nature
47 of the dispute. Whenever a statement of a dispute is filed, unless there
48 exists reasonable grounds to believe that it is wholly without merit,
49 the controller must note that it is disputed by the consumer and include
50 either the consumer's statement or a clear and accurate codification or
51 summary thereof with the disputed personal data whenever it is
52 disclosed, transferred, or sold to any processor or third party.
53   7. Right to delete. (a) Upon the verified request of a consumer, a
54 controller must:

(i) within forty-five days after receiving the verified request, delete any or all of the consumer's personal data, as directed by the consumer or their agent, that the controller possesses or controls; and
   (ii) unless it proves impossible or involves disproportionate effort that is documented in writing by the controller, communicate such request to each processor or third party to whom the controller disclosed, transferred or sold the personal data within one year preceding the consumer's request and to require those processors or third parties to do the same for any further processors or third parties they disclosed, transferred, or sold the personal data to.
   (b) For personal data that is not possessed by the controller but by a processor of the controller, the controller may choose to (i) communicate the consumer's request for deletion to the processor, or (ii) request that the processor return to the controller the personal data that is the subject of the consumer's request and delete such personal data upon receipt of the request.
   (c) A consumer's deletion of their online account must be treated as a request to the controller to delete all of that consumer's personal data directly related to that account.
   (d) A controller must maintain reasonable procedures designed to prevent the reappearance in its systems, and in any data it discloses, transfers, or sells to any processor or third party, the personal data 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 activities; or
   (ii) it is necessary for the controller to maintain the consumer's personal data to engage in public or peer-reviewed scientific, historical, 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.
   (f) Where a consumer's request for deletion is denied, the controller shall provide the consumer with a written justification for such denial.
   8. Responding to requests. (a) A controller must take action under subdivisions four through seven of this section and inform the consumer of any actions taken without undue delay and in any event within forty-five days of receipt of the request. That period may be extended once by forty-five additional days where reasonably necessary, taking into account the complexity and number of the requests. The controller must inform the consumer of any such extension within forty-five days of receipt of the request, together with the reasons for the delay. When a controller denies any such request, it must within this period disclose to the consumer a statement in writing of the specific reasons for the denial and instructions for how to appeal the decision.
   (b) A controller shall permit the exercise of rights and carry out its obligations set forth in subdivisions four through seven of this section free of charge, at least twice annually to the consumer. Where requests from a consumer are manifestly unfounded or excessive, in particular

because of their repetitive character, the controller may either (i)
charge a reasonable fee to cover the administrative costs of complying
with the request or (ii) refuse to act on the request and notify the
consumer of the reason for refusing the request. The controller bears
the burden of demonstrating the manifestly unfounded or excessive char-
acter of the request.
(c) (i) A controller shall promptly attempt, using commercially
reasonable efforts, to verify that all requests to exercise any rights
set forth in any section of this article requiring a verified request
were made by the consumer who is the subject of the data, or by a person
lawfully exercising the right on behalf of the consumer who is the
subject of the data. Commercially reasonable efforts shall be determined
based on the totality of the circumstances, including the nature of the
data implicated by the request.
(ii) A controller may require the consumer to provide additional
information only if the request cannot reasonably be verified without
the provision of such additional information. A controller must not
transfer or process any such additional information provided pursuant to
this section for any other purpose and must delete any such additional
information without undue delay and in any event within forty-five days
after the controller has notified the consumer that it has taken action
on a request under subdivisions four through seven of this section as
described in paragraph (a) of this subdivision.
(iii) If a controller discloses this additional information to any
processor or third party for the purpose of verifying a consumer
request, it must notify the receiving processor or third party at the
time of such disclosure, or as close in time to the disclosure as is
reasonably practicable, that such information was provided by the
consumer for the sole purpose of verification and cannot be processed
for any purpose other than verification.
9. Implementation of rights. Controllers must provide easily accessi-
ble and convenient means for consumers to exercise their rights under
this article.
10. Non-waiver of rights. Any provision of a contract or agreement of
any kind that purports to waive or limit in any way a consumer's rights
under this article is contrary to public policy and is void and unen-
forceable.
§ 1103. Controller, processor, and third party responsibilities. 1.
Controller responsibilities. (a) Data protection assessments. (i) A
controller shall regularly conduct and document a data protection
assessment for each of the controller's processing activities that
presents a heightened risk of harm to a consumer. For the purposes of
this section, processing that presents a heightened risk of harm to a
consumer includes: (A) the processing of personal data for the purposes
of targeting advertising, (B) the sale of personal data, (C) the proc-
essing of personal data for the purposes of profiling, where such
profiling presents a reasonably foreseeable risk of (I) unfair or decep-
tive treatment of, or unlawful disparate impact on consumers, (II)
financial, physical or reputational injury to consumers, (III) a phys-
ical or other intrusion upon the solitude or seclusion, or the private
affairs or concerns of consumers where such intrusion would be offensive
to a reasonable person, or (IV) other substantial injury to consumers;
and (D) the processing of sensitive data.
(ii) Data protection assessments conducted pursuant to subparagraph
(i) of this paragraph shall identify and weigh the benefits that may
flow, directly and indirectly, from the processing to the controller,

1   the consumer, other stakeholders and the public against the potential
2   risks to the rights of the consumer associated with such processing, as
3   mitigated by safeguards that can be employed by the controller to reduce
4   such risks. The controller shall factor into any such data protection
5   assessment that use of deidentified data and the reasonable expectations
6   of consumers, as well as the context of the processing and the relation-
7   ship between the controller and the consumer whose personal data will be
8   processed.
9   (iii) The attorney general may require that a controller disclose any
10   data   protection assessment that is relevant to an investigation
11   conducted by the attorney general, and the controller shall make the
12   data protection assessment available to the attorney general. The attor-
13   ney general may evaluate the data protection assessment to assess
14   compliance with the provisions of this article. Data protection assess-
15   ments shall be confidential and shall be exempt from disclosure under
16   the freedom of information law. To the extent any information contained
17   in a data protection assessment disclosure to the attorney general
18   includes information subject to attorney-client privilege or work prod-
19   uct protection, such disclosure shall not constitute a waiver of such
20   privilege or protection.
21   (iv) A single data protection assessment may address a comparable set
22   of processing operations that include similar activities.
23   (v) If a controller conducts a data protection assessment for the
24   purpose of complying with another applicable law or regulation, the data
25   protection assessment shall be deemed to satisfy the requirements estab-
26   lished in this section if such data protection assessment is reasonably
27   similar in scope and effect to the data protection assessment that would
28   otherwise be conducted pursuant to this section.
29   (vi) Data protection assessment requirements shall apply to processing
30   activities created or generated after the effective date of this arti-
31   cle.
32   (b) Controllers must not engage in unfair, deceptive, or abusive acts
33   or practices with respect to obtaining consumer consent, the processing
34   of personal data, and a consumer's exercise of any rights under this
35   article, including without limitation:
36   (i) designing a user interface with the purpose or substantial effect
37   of deceiving consumers, obscuring consumers' rights under this article,
38   or subverting or impairing user autonomy, decision-making, or choice; or
39   (ii) obtaining consent in a manner designed to overpower a consumer's
40   resistance; for example, by making excessive requests for consent.
41   (c) Controllers must develop, implement, and maintain reasonable safe-
42   guards to protect the security, confidentiality and integrity of the
43   personal data of consumers including adopting reasonable administrative,
44   technical and physical safeguards appropriate to the volume and nature
45   of the personal data at issue.
46   (d) (i) A controller shall limit the use and retention of a consumer's
47   personal data to what is (A) necessary to provide the services or goods
48   requested by the consumer, (B) necessary for the internal business oper-
49   ations of the controller and consistent with the disclosures made to the
50   consumer pursuant to section eleven hundred two of this article, or (C)
51   necessary to comply with the legal obligations of the controller.
52   (ii) At least annually, a controller shall review its retention prac-
53   tices for the purpose of ensuring that it is maintaining the minimum
54   amount of personal data as is necessary for the operation of its busi-
55   ness. A controller must securely dispose of all personal data that is no
56   longer (A) necessary to provide the services or goods requested by the

1 consumer, (B) necessary for the internal business operations of the
2 controller and consistent with the disclosures made to the consumer
3 pursuant to section eleven hundred two of this article, or (C) necessary
4 to comply with the legal obligations of the controller.
5   (e) Non-discrimination. (i) (A) A controller must not discriminate
6 against a consumer for exercising rights under this article, including
7 but not limited to, by:
8   (I) denying services or goods to consumers;
9   (II) charging different prices for services or goods, including
10 through the use of discounts or other benefits; imposing penalties; or
11 providing a different level or quality of services or goods to the
12 consumer; or
13   (III) suggesting that the consumer will receive a different price or
14 rate for services or goods or a different level or quality of services
15 or goods.
16   (B) A controller shall not be prohibited from offering a different
17 price, rate, level, quality, or selection of goods or services to a
18 consumer, including offering goods or services for no fee, if the offer-
19 ing is in connection with a consumer's voluntary participation in bona
20 fide loyalty, rewards, premium features, discounts, or club card
21 program. If a consumer exercises their right pursuant to paragraph (a)
22 of subdivision two of section eleven hundred two of this article, a
23 controller may not sell personal data to a third party controller as
24 part of such a program unless: (I) the sale is reasonably necessary to
25 enable the third party to provide a benefit to which the consumer is
26 entitled; (II) the sale of personal data to third parties is clearly
27 disclosed in the terms of the program; and (III) the third party uses
28 the personal data only for purposes of facilitating such a benefit to
29 which the consumer is entitled and does not retain or otherwise use or
30 disclose the personal data for any other purpose.
31   (ii) This paragraph does not apply to a controller's conduct with
32 respect to opt-in consent, in which case paragraph (j) of subdivision
33 three of section eleven hundred two of this article governs.
34   (f) Agreements with processors. (i) Before making any disclosure,
35 transfer, or sale of personal data to any processor, the controller must
36 enter into a written, signed contract with that processor. Such contract
37 must be binding and clearly set forth instructions for processing data,
38 the nature and purpose of processing, the type of data subject to proc-
39 essing, the duration of processing, and the rights and obligations of
40 both parties. The contract must also include requirements that the
41 processor must:
42   (A) ensure that each person processing personal data is subject to a
43 duty of confidentiality with respect to the data;
44   (B) protect the data in a manner consistent with the requirements of
45 this article and at least equal to the security requirements of the
46 controller set forth in their publicly available policies, notices, or
47 similar statements;
48   (C) process the data only when and to the extent necessary to comply
49 with its legal obligations to the controller unless otherwise explicitly
50 authorized by the controller;
51   (D) not combine the personal data which the processor receives from or
52 on behalf of the controller with personal data which the processor
53 receives from or on behalf of another person or collects from its own
54 interaction with consumers;
55   (E) comply with any exercises of a consumer's rights under section
56 eleven hundred two of this article upon the request of the controller,

1 subject to the limitations set forth in section eleven hundred five of
2 this article;
3 (F) at the controller's direction, delete or return all personal data
4 to the controller as requested at the end of the provision of services,
5 unless retention of the personal data is required by law;
6 (G) upon the reasonable request of the controller, make available to
7 the controller all data in its possession necessary to demonstrate the
8 processor's compliance with the obligations in this article;
9 (H) allow, and cooperate with, reasonable assessments by the control-
10 ler or the controller's designated assessor; alternatively, the process-
11 or may arrange for a qualified and independent assessor to conduct an
12 assessment of the processor's policies and technical and organizational
13 measures in support of the obligations under this article using an
14 appropriate and accepted control standard or framework and assessment
15 procedure for such assessments. The processor shall provide a report of
16 such assessment to the controller upon request;
17 (I) a reasonable time in advance before disclosing or transferring the
18 data to any further processors, notify the controller of such a proposed
19 disclosure or transfer and provide the controller an opportunity to
20 approve or reject the proposal; and
21 (J) engage any further processor pursuant to a written, signed
22 contract that includes the contractual requirements provided in this
23 paragraph, containing at minimum the same obligations that the processor
24 has entered into with regard to the data.
25 (ii) A controller must not agree to indemnify, defend, or hold a
26 processor harmless, or agree to a provision that has the effect of
27 indemnifying, defending, or holding the processor harmless, from claims
28 or liability arising from the processor's breach of the contract
29 required by clause (A) of subparagraph (i) of this paragraph or a
30 violation of this article. Any provision of an agreement that violates
31 this subparagraph is contrary to public policy and is void and unen-
32 forceable.
33 (iii) Nothing in this paragraph relieves a controller or a processor
34 from the liabilities imposed on it by virtue of its role in the process-
35 ing relationship as defined by this article.
36 (iv) Determining whether a person is acting as a controller or proces-
37 sor with respect to a specific processing of data is a fact-based deter-
38 mination that depends upon the context in which personal data is to be
39 processed. A processor that continues to adhere to a controller's
40 instructions with respect to a specific processing of personal data
41 remains a processor.
42 (g) Third parties. (i) A controller must not share, disclose, trans-
43 fer, or sell personal data, or facilitate or enable the processing,
44 disclosure, transfer, or sale to a third party of personal data for
45 which a consumer has exercised their opt-out rights pursuant to subdivi-
46 sion two of section eleven hundred two of this article, or for which
47 consent of the consumer pursuant to subdivision three of section eleven
48 hundred two of this article, has not been obtained or is not currently
49 in effect. Any request for consent to share, disclose, transfer, or sell
50 personal data, or to facilitate or enable the processing, disclosure,
51 transfer, or sale of personal data to a third party of personal data to
52 a third party must clearly include the category of the third party and
53 the processing purposes for which the third party may use the personal
54 data.
55 (ii) A controller must not share, disclose, transfer, or sell personal
56 data, or facilitate or enable the processing, disclosure, transfer, or

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

1   (b) The processing is made pursuant to a request by a federal, state,
2   or local government or government entity; or
3   (c) The processing significantly advances protection against criminal
4   or tortious activity.
5   § 1104. Data brokers. 1. A data broker, as defined under this article,
6   must annually, on or before January thirty-first following a year in
7   which a person meets the definition of data broker in this article:
8   (a) Register with the attorney general;
9   (b) Pay a registration fee of one hundred dollars or as otherwise
10   determined by the attorney general pursuant to the regulatory authority
11   granted to the attorney general under this article, not to exceed the
12   reasonable cost of establishing and maintaining the database and infor-
13   mational website described in this section; and
14   (c) Provide the following information:
15   (i) the name and primary physical, email, and internet website address
16   of the data broker;
17   (ii) the name and business address of an officer or registered agent
18   of the data broker authorized to accept legal process on behalf of the
19   data broker;
20   (iii) a statement describing the method for exercising consumers
21   rights under section eleven hundred two of this article;
22   (iv) a statement whether the data broker implements a purchaser
23   credentialing process; and
24   (v) any additional information or explanation the data broker chooses
25   to provide concerning its data collection practices.
26   2. Notwithstanding any other provision of this article, any controller
27   that conducts business in the state of New York must:
28   (a) annually, on or before January thirty-first following a year in
29   which a person meets the definition of controller in this act, provide
30   to the attorney general a list of all data brokers or persons reasonably
31   believed to be data brokers to which the controller provided personal
32   data in the preceding year; and
33   (b) not sell a consumer's personal data to an entity reasonably
34   believed to be a data broker that is not registered with the attorney
35   general.
36   3. The attorney general shall establish, manage and maintain a state-
37   wide registry on its internet website, which shall list all registered
38   data brokers and make accessible to the public all the information
39   provided by data brokers pursuant to this section. Printed hard copies
40   of such registry shall be made available upon request and payment of a
41   reasonable fee to be determined by the attorney general.
42   4. A data broker that fails to register as required by this section or
43   submits false information in its registration is, in addition to any
44   other injunction, penalty, or liability that may be imposed under this
45   article, liable for civil penalties, fees, and costs in an action
46   brought by the attorney general as follows: (a) a civil penalty of one
47   thousand dollars for each day the data broker fails to register as
48   required by this section or fails to correct false information, (b) an
49   amount equal to the fees that were due during the period it failed to
50   register, and (c) expenses incurred by the attorney general in the
51   investigation and prosecution of the action as the court deems appropri-
52   ate.
53   § 1105. Limitations. 1. This article does not require a controller or
54   processor to do any of the following solely for purposes of complying
55   with this article:
56   (a) Reidentify deidentified data;

 (b) Comply with a verified consumer request to access, correct, or
delete personal data pursuant to this article if all of the following
are true:
 (i) The controller is not reasonably capable of associating the
request with the personal data;
 (ii) The controller does not associate the personal data with other
personal data about the same specific consumer as part of its normal
business practice; and
 (iii) The controller does not sell the personal data to any third
party or otherwise voluntarily disclose or transfer the personal data to
any processor or third party, except as otherwise permitted in this
article; or
 (c) Maintain personal data in identifiable form, or collect, obtain,
retain, or access any personal data or technology, in order to be capa-
ble of associating a verified consumer request with personal data.
 2. The obligations imposed on controllers and processors under this
article do not restrict a controller's or processor's ability to do any
of the following, to the extent that the use of the consumer's personal
data is reasonably necessary and proportionate for these purposes:
 (a) Comply with federal, state, or local laws, rules, or regulations,
provided that no law enforcement agency or officer thereof shall access
personal data without a lawfully executed search warrant, except for the
attorney general for the purposes of enforcing this article, except
where otherwise provided specifically in federal law;
 (b) Investigate, establish, exercise, prepare for, or defend legal
claims;
 (c) Process personal data necessary to provide the services or goods
requested by a consumer; perform a contract to which the consumer is a
party; or take steps at the request of the consumer prior to entering
into a contract;
 (d) 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;
 (e) 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;
 (f) Identify and repair technical errors that impair existing or
intended functionality; or
 (g) 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 four
through seven of section eleven hundred two of this article, or a
processor or third party to whom a controller communicates such a
request, may decline to fulfill the relevant part of such request if:

 1 (a) the controller, processor, or third party is unable to verify the
 2 request using commercially reasonable efforts, as described in paragraph
 3 (c) of subdivision eight of section eleven hundred two of this article;
 4 (b) complying with the request would be demonstrably impossible (for
 5 purposes of this paragraph, the receipt of a large number of verified
 6 requests, on its own, is not sufficient to render compliance with a
 7 request demonstrably impossible);
 8 (c) complying with the request would impair the privacy of another
 9 individual or the rights of another to exercise free speech; or
10 (d) the personal data was created by a natural person other than the
11 consumer making the request and is being processed for the purpose of
12 facilitating interpersonal relationships or public discussion.
13 § 1106. Enforcement. 1. Whenever it appears to the attorney general,
14 either upon complaint or otherwise, that any person or persons has
15 engaged in or is about to engage in any of the acts or practices stated
16 to be unlawful under this article, the attorney general may bring an
17 action or special proceeding in the name and on behalf of the people of
18 the state of New York to enjoin any violation of this article, to obtain
19 restitution of any moneys or property obtained directly or indirectly by
20 any such violation, to obtain disgorgement of any profits obtained
21 directly or indirectly by any such violation, to obtain civil penalties
22 of not more than twenty thousand dollars per violation, and to obtain
23 any such other and further relief as the court may deem proper, includ-
24 ing preliminary relief.
25 (a) Any action or special proceeding brought by the attorney general
26 pursuant to this section must be commenced within six years.
27 (b) Each instance of unlawful processing counts as a separate
28 violation. Unlawful processing of the personal data of more than one
29 consumer counts as a separate violation as to each consumer. Each
30 provision of this article that is violated counts as a separate
31 violation.
32 (c) In assessing the amount of penalties, the court must consider any
33 one or more of the relevant circumstances presented by any of the
34 parties, including, but not limited to, the nature and seriousness of
35 the misconduct, the number of violations, the persistence of the miscon-
36 duct, the length of time over which the misconduct occurred, the will-
37 fulness of the violator's misconduct, and the violator's financial
38 condition.
39 2. In connection with any proposed action or special proceeding under
40 this section, the attorney general is authorized to take proof and make
41 a determination of the relevant facts, and to issue subpoenas in accord-
42 ance with the civil practice law and rules. The attorney general may
43 also require such other data and information as he or she may deem rele-
44 vant and may require written responses to questions under oath. Such
45 power of subpoena and examination shall not abate or terminate by reason
46 of any action or special proceeding brought by the attorney general
47 under this article.
48 3. Any person, within or outside the state, who the attorney general
49 believes may be in possession, custody, or control of any books, papers,
50 or other things, or may have information, relevant to acts or practices
51 stated to be unlawful in this article is subject to the service of a
52 subpoena issued by the attorney general pursuant to this section.
53 Service may be made in any manner that is authorized for service of a
54 subpoena or a summons by the state in which service is made.
55 4. (a) Failure to comply with a subpoena issued pursuant to this
56 section without reasonable cause tolls the applicable statutes of limi-

1 tations in any action or special proceeding brought by the attorney
2 general against the noncompliant person that arises out of the attorney
3 general's investigation.
4 (b) If a person fails to comply with a subpoena issued pursuant to
5 this section, the attorney general may move in the supreme court to
6 compel compliance. If the court finds that the subpoena was authorized,
7 it shall order compliance and may impose a civil penalty of up to one
8 thousand dollars per day of noncompliance.
9 (c) Such tolling and civil penalty shall be in addition to any other
10 penalties or remedies provided by law for noncompliance with a subpoena.
11 5. This section shall apply to all acts declared to be unlawful under
12 this article, whether or not subject to any other law of this state, and
13 shall not supersede, amend or repeal any other law of this state under
14 which the attorney general is authorized to take any action or conduct
15 any inquiry.
16 § 1107. Miscellaneous. 1. Preemption: This article does not annul,
17 alter, or affect the laws, ordinances, regulations, or the equivalent
18 adopted by any local entity regarding the processing, collection, trans-
19 fer, disclosure, and sale of consumers' personal data by a controller or
20 processor subject to this article, except to the extent those laws,
21 ordinances, regulations, or the equivalent create requirements or obli-
22 gations that conflict with or reduce the protections afforded to consum-
23 ers under this article.
24 2. Impact report: The attorney general shall issue a report evaluating
25 this article, its scope, any complaints from consumers or persons, the
26 liability and enforcement provisions of this article including, but not
27 limited to, the effectiveness of its efforts to enforce this article,
28 and any recommendations for changes to such provisions. The attorney
29 general shall submit the report to the governor, the temporary president
30 of the senate, the speaker of the assembly, and the appropriate commit-
31 tees of the legislature within two years of the effective date of this
32 section.
33 3. Regulatory authority: (a) The attorney general is hereby authorized
34 and empowered to adopt, promulgate, amend and rescind suitable rules and
35 regulations to carry out the provisions of this article, including rules
36 governing the form and content of any disclosures or communications
37 required by this article.
38 (b) The attorney general may request, and shall receive, data and
39 information from controllers conducting business in New York state,
40 other New York state government entities administering notice and
41 consent regimes, consumer protection and privacy advocates and research-
42 ers, internet standards setting bodies, such as the internet engineering
43 taskforce and the institute of electrical and electronics engineers, and
44 other relevant sources, to conduct studies to inform suitable rules and
45 regulations. The attorney general shall receive, upon request, data
46 from other New York state governmental entities.
47 4. Exercise of rights: Any consumer right set forth in this article
48 may be exercised at any time by the consumer who is the subject of the
49 data or by a parent or guardian authorized by law to take actions of
50 legal consequence on behalf of the consumer who is the subject of the
51 data. An agent authorized by a consumer may exercise the consumer rights
52 set forth in subdivisions four through seven of section eleven hundred
53 two of this article on the consumers behalf.
54 § 4. Severability. If any provision of this act, or any application of
55 any provision of this act, is held to be invalid, that shall not affect
56 the validity or effectiveness of any other provision of this act, or of

1 any other application of any provision of this act, which can be given
2 effect without that provision or application; and to that end, the
3 provisions and applications of this act are severable.
4   § 5. This act shall take effect immediately; provided, however, that
5 sections 1101, 1102, 1103, 1105, 1106 and 1107 of the general business
6 law, as added by section three of this act, shall take effect one year
7 after it shall have become a law.