

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

H.211

An act relating to data brokers and personal information

It is hereby enacted by the General Assembly of the State of Vermont:

Sec. 1. 9 V.S.A. chapter 62 is amended to read:

CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

Subchapter 1. General Provisions

§ 2430. DEFINITIONS

As used in this chapter:

(1) “Authorized agent” means:

(A) a person designated by a consumer to act on the consumer’s behalf;

(B) a parent or legal guardian that acts on behalf of the parent’s child or on behalf of a child for whom the guardian has legal responsibility; or

(C) a guardian or conservator that acts on behalf of a consumer that is subject to a guardianship, conservatorship, or other protective arrangement.

(2)(A) “Biometric data” means that data generated from the technological processing of an individual’s unique biological, physical, or physiological characteristics can be used to identify an individual, including:

(i) iris or retina scans;

(ii) fingerprints;

(iii) facial or hand mapping, geometry, or templates;

- 1 (iv) vein patterns;
2 (v) voice prints; and
3 (vi) gait or personally identifying physical movement or patterns.

4 (B) “Biometric data” does not include:

- 5 (i) a digital or physical photograph;
6 (ii) an audio or video recording; or
7 (iii) any data generated from a digital or physical photograph, or
8 an audio or video recording, unless such data is generated to identify a specific
9 individual.

10 (3)(A) “Brokered personal information” means ~~one or more of the~~
11 ~~following computerized data elements about a consumer, if categorized or~~
12 ~~organized for dissemination to third parties:~~

- 13 ~~(i) name;~~
14 ~~(ii) address;~~
15 ~~(iii) date of birth;~~
16 ~~(iv) place of birth;~~
17 ~~(v) mother’s maiden name;~~
18 ~~(vi) unique biometric data generated from measurements or~~
19 ~~technical analysis of human body characteristics used by the owner or licensee~~
20 ~~of the data to identify or authenticate the consumer, such as a fingerprint, retina~~

1 ~~or iris image, or other unique physical representation or digital representation~~
2 ~~of biometric data;~~

3 ~~(vii) name or address of a member of the consumer's immediate~~
4 ~~family or household;~~

5 ~~(viii) Social Security number or other government issued~~
6 ~~identification number; or~~

7 ~~(ix) other information that, alone or in combination with the other~~
8 ~~information sold or licensed, would allow a reasonable person to identify the~~
9 ~~consumer with reasonable certainty~~ any information, including derived data
10 and unique identifiers, that is linked or reasonably linkable, alone or in
11 combination with other information, to an identified or identifiable individual
12 or to a device that identifies, is linked to, or is reasonably linkable to one or
13 more identified or identifiable individuals in a household.

14 (B) "Brokered personal information" does not include publicly
15 available information ~~to the extent that it is related to a consumer's business or~~
16 ~~profession.~~

17 ~~(2)(4)~~ "Business" means a commercial entity, including a sole
18 proprietorship, partnership, corporation, association, limited liability company,
19 or other group, however organized and whether or not organized to operate at a
20 profit, including a financial institution organized, chartered, or holding a
21 license or authorization certificate under the laws of this State, any other state,

1 the United States, or any other country, or the parent, affiliate, or subsidiary of
2 a financial institution, but does not include the State, a State agency, any
3 political subdivision of the State, or a vendor acting solely on behalf of, and at
4 the direction of, the State.

5 ~~(3)~~(5) “Consumer” means an individual residing in this State.

6 ~~(4)~~(6)(A) “Data broker” means a business, or unit or units of a business,
7 separately or together, that knowingly collects and sells or licenses to third
8 parties the brokered personal information of a consumer with whom the
9 business does not have a direct relationship.

10 (B) ~~Examples of a direct relationship with a business include if the~~
11 ~~consumer is a past or present:~~

12 ~~(i) customer, client, subscriber, user, or registered user of the~~
13 ~~business’s goods or services;~~

14 ~~(ii) employee, contractor, or agent of the business;~~

15 ~~(iii) investor in the business; or~~

16 ~~(iv) donor to the business~~ As used in this subdivision (6), “direct
17 relationship” means that a consumer has intentionally interacted with a
18 business for the purpose of accessing, purchasing, using, requesting, or
19 obtaining information about the business’s products or services. A consumer
20 does not have a direct relationship with a business if the purpose of the
21 consumer’s engagement is to exercise a consumer right or for the business to

1 verify the consumer's identity. A business does not have a direct relationship
2 with a consumer simply because the business collects brokered personal
3 information directly from the consumer; the consumer must intend to interact
4 with the business. A business is still a data broker and does not have a direct
5 relationship with a consumer as to the brokered personal information the
6 business sells about the consumer that it collected outside of a first-party
7 interaction with the consumer.

8 ~~(C) The following activities conducted by a business, and the~~
9 ~~collection and sale or licensing of brokered personal information incidental to~~
10 ~~conducting these activities, do not qualify the business as a data broker:~~

11 ~~(i) developing or maintaining third party e-commerce or~~
12 ~~application platforms;~~

13 ~~(ii) providing 411 directory assistance or directory information~~
14 ~~services, including name, address, and telephone number, on behalf of or as a~~
15 ~~function of a telecommunications carrier;~~

16 ~~(iii) providing publicly available information related to a~~
17 ~~consumer's business or profession; or~~

18 ~~(iv) providing publicly available information via real time or near-~~
19 ~~real time alert services for health or safety purposes.~~

1 ~~(D)~~(C) The phrase “sells or licenses” does not include:

2 ~~(i)~~ a one-time or occasional sale of assets of a business as part of a
3 transfer of control of those assets that is not part of the ordinary conduct of the
4 business; ~~or~~

5 ~~(ii)~~ a sale or license of data that is merely incidental to the
6 business.

7 ~~(5)(A)~~ “Data broker security breach” means an unauthorized acquisition
8 or a reasonable belief of an unauthorized acquisition of more than one element
9 of brokered personal information maintained by a data broker when the
10 brokered personal information is not encrypted, redacted, or protected by
11 another method that renders the information unreadable or unusable by an
12 unauthorized person.

13 ~~(B)~~ “Data broker security breach” does not include good faith but
14 unauthorized acquisition of brokered personal information by an employee or
15 agent of the data broker for a legitimate purpose of the data broker, provided
16 that the brokered personal information is not used for a purpose unrelated to
17 the data broker’s business or subject to further unauthorized disclosure.

18 ~~(C)~~ In determining whether brokered personal information has been
19 acquired or is reasonably believed to have been acquired by a person without
20 valid authorization, a data broker may consider the following factors, among
21 others:

1 ~~(i) indications that the brokered personal information is in the~~
2 ~~physical possession and control of a person without valid authorization, such~~
3 ~~as a lost or stolen computer or other device containing brokered personal~~
4 ~~information;~~

5 ~~(ii) indications that the brokered personal information has been~~
6 ~~downloaded or copied;~~

7 ~~(iii) indications that the brokered personal information was used~~
8 ~~by an unauthorized person, such as fraudulent accounts opened or instances of~~
9 ~~identity theft reported; or~~

10 ~~(iv) that the brokered personal information has been made public.~~

11 ~~(6)~~(7) “Data collector” means a person who, for any purpose, whether
12 by automated collection or otherwise, handles, collects, disseminates, or
13 otherwise deals with personally identifiable information, and includes the
14 State, State agencies, political subdivisions of the State, public and private
15 universities, privately and publicly held corporations, limited liability
16 companies, financial institutions, and retail operators.

17 ~~(7)~~(8) “Encryption” means use of an algorithmic process to transform
18 data into a form in which the data is rendered unreadable or unusable without
19 use of a confidential process or key.

1 ~~(9)~~(A) “GenAI system” means an artificial intelligence system that can
2 generate derived synthetic content, including text, images, video, and audio,
3 that emulates the structure and characteristics of the system’s training data.

4 (B) As used in subdivision (A) of this subdivision (9), “artificial
5 intelligence system” means an engineered or machine-based system that varies
6 in its level of autonomy and that can, for explicit or implicit objectives, infer
7 from the input it receives how to generate outputs that can influence physical
8 or virtual environments.

9 (10) “Identified or identifiable individual” means an individual who can
10 be readily identified, directly or indirectly.

11 ~~(8)~~(11) “License” means a grant of access to, or distribution of, data by
12 one person to another in exchange for consideration. A use of data for the sole
13 benefit of the data provider, where the data provider maintains control over the
14 use of the data, is not a license.

15 ~~(9)~~(12) “Login credentials” means a consumer’s user name or ~~e-mail~~
16 email address, in combination with a password or an answer to a security
17 question, that together permit access to an online account.

18 ~~(40)~~(13)(A) “Personally identifiable information” means a consumer’s
19 first name or first initial and last name in combination with one or more of the
20 following digital data elements, when the data elements are not encrypted,
21 redacted, or protected by another method that renders them unreadable or

1 unusable by unauthorized persons, subject to the exception in subdivision (C)
2 of this subdivision (13):

3 (i) a Social Security number;

4 (ii) a driver license or nondriver State identification card number,
5 individual taxpayer identification number, passport number, military
6 identification card number, or other identification number that originates from
7 a government identification document that is commonly used to verify identity
8 for a commercial transaction;

9 (iii) a financial account number or credit or debit card number, if
10 the number could be used without additional identifying information, access
11 codes, or passwords;

12 (iv) a password, personal identification number, or other access
13 code for a financial account;

14 (v) ~~unique biometric data generated from measurements or~~
15 ~~technical analysis of human body characteristics used by the owner or licensee~~
16 ~~of the data to identify or authenticate the consumer, such as a fingerprint, retina~~
17 ~~or iris image, or other unique physical representation or digital representation~~
18 ~~of biometric data;~~

19 (vi) genetic information; and

20 (vii)(I) health records or records of a wellness program or similar
21 program of health promotion or disease prevention;

1 (II) a health care professional’s medical diagnosis or treatment
2 of the consumer; or

3 (III) a health insurance policy number.

4 (B) “Personally identifiable information” does not ~~mean~~ include
5 publicly available information ~~that is lawfully made available to the general~~
6 ~~public from federal, State, or local government records.~~

7 (C) “Personally identifiable information” does not require a
8 consumer’s first name or first initial and last name if any of the data elements
9 contained in subdivisions (A)(i)–(vii) of this subdivision (13) is sufficient to
10 perform or attempt to perform identity theft against the consumer.

11 (14) “Precise geolocation” means information derived from technology
12 that can precisely and accurately identify the specific location of a consumer
13 within a radius of 1,850 feet.

14 (15) “Processor” means a person who performs any operation or set of
15 operations, whether by manual or automated means, on brokered personal
16 information or on sets of brokered personal information, such as the collection,
17 use, storage, disclosure, analysis, deletion, or modification of brokered
18 personal information on behalf of a business.

19 (16)(A) “Publicly available information” means information that:

20 (i) is made available:

21 (I) through federal, state, or local government records; or

1 (II) to the general public from widely distributed media; or

2 (ii) a data broker has a reasonable basis to believe that the

3 consumer has lawfully made available to the general public.

4 (B) “Publicly available information” does not include:

5 (i) biometric data collected by a business about a consumer

6 without the consumer’s knowledge;

7 (ii) information that is collated and combined to create a consumer

8 profile that is made available to a user of a publicly available website either in

9 exchange for payment or free of charge;

10 (iii) information that is made available for sale;

11 (iv) an inference about a consumer that is generated from the

12 information described in subdivision (ii) or (iii) of this subdivision (16)(B);

13 (v) any obscene visual depiction, as defined in 18 U.S.C. § 1460;

14 (vi) brokered personal information that is created through the

15 combination of brokered personal information with publicly available

16 information;

17 (vii) genetic data, unless otherwise made publicly available by the

18 consumer to whom the information pertains;

19 (viii) information provided by a consumer on a website or online

20 service made available to all members of the public, for free or for a fee, where

1 the consumer has maintained a reasonable expectation of privacy in the
2 information, such as by restricting the information to a specific audience; or

3 (ix) intimate images, authentic or computer-generated, known to
4 be nonconsensual.

5 ~~(14)~~(17) “Record” means any material on which written, drawn, spoken,
6 visual, or electromagnetic information is recorded or preserved, regardless of
7 physical form or characteristics.

8 ~~(12)~~(18) “Redaction” means the rendering of data so that the data are
9 unreadable or are truncated so that ~~no~~ not more than the last four digits of the
10 identification number are accessible as part of the data.

11 (19)(A) “Sale” means the exchange of a consumer’s brokered personal
12 information by the data broker to a third party for monetary or other valuable
13 consideration.

14 (B) “Sale” does not include:

15 (i) the disclosure of brokered personal information to a processor
16 that processes the brokered personal information on behalf of the data broker;

17 (ii) the disclosure of brokered personal information to a third party
18 for purposes of providing a product or service requested by the consumer;

19 (iii) the disclosure or transfer of brokered personal information to
20 an affiliate of the data broker;

1 (iv) the disclosure, with the consumer’s consent, of brokered
2 personal information where the consumer directs the data broker to disclose the
3 brokered personal information or intentionally uses the data broker to interact
4 with a third party;

5 (v) the disclosure of publicly available information; or

6 (vi) the disclosure or transfer of brokered personal information to
7 a third party as an asset that is part of a merger, acquisition, bankruptcy, or
8 other transaction, or a proposed merger, acquisition, bankruptcy, or other
9 transaction, in which the third party assumes control of all or part of the data
10 broker’s assets.

11 (C) As used in subdivision (B) of this subdivision (19), “affiliate”
12 means a legal entity that shares common branding with another legal entity or
13 controls, is controlled by, or is under common control with another legal entity.

14 (D) As used in subdivision (C) of this subdivision (19), “control” or
15 “controlled” means:

16 (i) ownership of, or the power to vote, more than 50 percent of the
17 outstanding shares of any class of voting security of a company;

18 (ii) control in any manner over the election of a majority of the
19 directors or of individuals exercising similar functions; or

20 (iii) the power to exercise controlling influence over the
21 management of a company.

1 ~~(13)~~(20)(A) “Security breach” means unauthorized acquisition of
2 electronic data, or a reasonable belief of an unauthorized acquisition of
3 electronic data, that compromises the security, confidentiality, or integrity of a
4 consumer’s personally identifiable information or login credentials maintained
5 by a data collector.

6 (B) “Security breach” does not include good faith but unauthorized
7 acquisition of personally identifiable information or login credentials by an
8 employee or agent of the data collector for a legitimate purpose of the data
9 collector, provided that the personally identifiable information or login
10 credentials are not used for a purpose unrelated to the data collector’s business
11 or subject to further unauthorized disclosure.

12 (C) In determining whether personally identifiable information or
13 login credentials have been acquired or ~~is~~ are reasonably believed to have been
14 acquired by a person without valid authorization, a data collector may consider
15 the following factors, among others:

16 (i) indications that the information is in the physical possession
17 and control of a person without valid authorization, such as a lost or stolen
18 computer or other device containing information;

19 (ii) indications that the information has been downloaded or
20 copied;

1 (iii) indications that the information was used by an unauthorized
2 person, such as fraudulent accounts opened or instances of identity theft
3 reported; or

4 (iv) that the information has been made public.

5 § 2431. ACQUISITION AND DISCLOSURE OF BROKERED PERSONAL
6 INFORMATION; PROHIBITIONS

7 (a) Prohibited acquisition and use.

8 (1) A person shall not acquire brokered personal information through
9 fraudulent means.

10 (2) A person shall not acquire or use brokered personal information for
11 the purpose of:

12 (A) stalking or harassing another person;

13 (B) committing a fraud, including identity theft, financial fraud, or e-
14 ~~mail~~ email fraud; or

15 (C) engaging in unlawful discrimination, including employment
16 discrimination and housing discrimination.

17 (b) Disclosure. A data broker shall:

18 (1) maintain procedures that require prospective users of the data
19 broker's brokered personal information to identify themselves, state the
20 purposes for which the information is sought, and certify that the information
21 shall be used for no other purpose;

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

* * *

(6) A data collector may provide notice of a security breach involving personally identifiable information to a consumer by one or more of the following methods:

(A) Direct notice, which may be by one of the following methods:

(i) written notice mailed to the consumer's residence;

(ii) electronic notice, for those consumers for whom the data collector has a valid ~~e-mail~~ email address, if:

(I) the data collector's primary method of communication with the consumer is by electronic means, the electronic notice does not request or contain a hypertext link to a request that the consumer provide personal information, and the electronic notice conspicuously warns consumers not to provide personal information in response to electronic communications regarding security breaches; or

(II) the notice is consistent with the provisions regarding electronic records and signatures for notices in 15 U.S.C. § 7001; or

(iii) telephonic notice, for those consumers for whom the data collector has a valid phone number, provided that the telephonic contact is made directly with each affected consumer and not through a prerecorded message and further provided that the data collector makes not less than five

1 attempts to contact the consumer for a live conversation before the data
2 collector may leave a voicemail providing information about the breach.

3 * * *

4 (c) Notice to consumer reporting agencies. In the event a data collector
5 provides notice to more than 1,000 consumers at one time pursuant to this
6 section, the data collector shall notify, without unreasonable delay, all
7 consumer reporting agencies that compile and maintain files on consumers on
8 a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing,
9 distribution, and content of the notice. This subsection shall not apply to a
10 person who is licensed or registered under Title 8 by the Department of
11 Financial Regulation.

12 (d) Exception to notice requirement.

13 (1) Notice of a security breach pursuant to subsection (b) of this section
14 is not required if the data collector establishes that misuse of personally
15 identifiable information or login credentials is not reasonably possible and the
16 data collector provides notice of the determination that the misuse of the
17 personally identifiable information or login credentials is not reasonably
18 possible pursuant to the requirements of this subsection. If the data collector
19 establishes that misuse of the personally identifiable information or login
20 credentials is not reasonably possible, the data collector shall provide notice of
21 its determination that misuse of the personally identifiable information or login

1 credentials is not reasonably possible and a detailed explanation for said
2 determination to the Vermont Attorney General or to the Department of
3 Financial Regulation in the event that the data collector is a person or entity
4 licensed or registered with the Department under Title 8 or this title. The data
5 collector may designate its notice and detailed explanation to the Vermont
6 Attorney General or the Department of Financial Regulation as “trade secret”
7 if the notice and detailed explanation meet the definition of trade secret
8 contained in 1 V.S.A. § 317(c)(9).

9 * * *

10 (e) HIPAA compliance. A data collector that is subject to the privacy,
11 security, and breach notification rules adopted in 45 C.F.R. Part 164 pursuant
12 to the federal Health Insurance Portability and Accountability Act, P.L. 104-
13 191 (1996) is deemed to be in compliance with this subchapter if the data
14 collector:

15 (1) ~~the data collector~~ experiences a security breach that is limited to
16 personally identifiable information specified in subdivision 2430(10)(A)(vii) of
17 this chapter; ~~and~~

18 (2) ~~the data collector~~ provides notice to affected consumers pursuant to
19 the requirements of the breach notification rule in 45 C.F.R. Part 164, Subpart
20 D; and

1 § 2436. NOTICE OF DATA BROKER SECURITY BREACHES

2 (a) Short title and definitions.

3 (1) This section shall be known as the “Data Broker Security Breach
4 Notice Act.”

5 (2)(A) As used in this section, “data broker security breach” means an
6 unauthorized acquisition or a reasonable belief of an unauthorized acquisition
7 of more than one instance of brokered personal information maintained by a
8 data broker when the brokered personal information is not encrypted, redacted,
9 or protected by another method that renders the information unreadable or
10 unusable by an unauthorized person.

11 (B) “Data broker security breach” does not include good faith but
12 unauthorized acquisition of brokered personal information by an employee or
13 agent of the data broker for a legitimate purpose of the data broker, provided
14 that the brokered personal information is not used for a purpose unrelated to
15 the data broker’s business or subject to further unauthorized disclosure.

16 (C) In determining whether brokered personal information has been
17 acquired or is reasonably believed to have been acquired by a person without
18 valid authorization, a data broker may consider the following factors, among
19 others:

20 (i) indications that the brokered personal information is in the
21 physical possession and control of a person without valid authorization, such

1 as a lost or stolen computer or other device containing brokered personal
2 information;

3 (ii) indications that the brokered personal information has been
4 downloaded or copied;

5 (iii) indications that the brokered personal information was used
6 by an unauthorized person, such as fraudulent accounts opened or instances of
7 identity theft reported; or

8 (iv) that the brokered personal information has been made public.

9 (b) Notice of breach.

10 (1) Except as otherwise provided in subsection (c) of this section, a data
11 broker shall, following discovery or notification to the data broker of a security
12 breach affecting a consumer, notify the consumer that there has been a data
13 broker security breach. Notice of the security breach shall be made in the most
14 expedient time possible and without unreasonable delay, but not later than 45
15 days after the discovery or notification, consistent with the legitimate needs of
16 the law enforcement agency, as provided in subdivisions (3) and (4) of this
17 subsection, or with any measures necessary to determine the scope of the
18 security breach and restore the reasonable integrity, security, and
19 confidentiality of the data system.

20 (2) A data broker shall provide notice of a breach to the Attorney

21 General as follows:

1 (A)(i) The data broker shall notify the Attorney General of the date of
2 the security breach and the date of discovery of the breach and shall provide a
3 preliminary description of the breach within 14 business days, consistent with
4 the legitimate needs of the law enforcement agency, as provided in
5 subdivisions (3) and (4) of this subsection (b), after the data broker's discovery
6 of the security breach.

7 (ii) If the date of the breach is unknown at the time notice is sent
8 to the Attorney General, the data broker shall send the Attorney General the
9 date of the breach as soon as it is known.

10 (iii) Unless otherwise ordered by a court of this State for good
11 cause shown, a notice provided under this subdivision (2)(A) shall not be
12 disclosed, without the consent of the data broker, to any person other than the
13 authorized agent or representative of the Attorney General, a State's Attorney,
14 or another law enforcement officer engaged in legitimate law enforcement
15 activities.

16 (B)(i) When the data broker provides notice of the breach pursuant to
17 subdivision (1) of this subsection (b), the data broker shall notify the Attorney
18 General of the number of Vermont consumers affected, if known to the data
19 broker, and shall provide a copy of the notice provided to consumers under
20 subdivision (1) of this subsection (b).

1 (ii) The data broker may send to the Attorney General a second
2 copy of the consumer notice, from which is redacted the type of brokered
3 personal information that was subject to the breach, that the Attorney General
4 shall use for any public disclosure of the breach.

5 (3) The notice to the Attorney General and a consumer required by this
6 subsection shall be delayed upon request of a law enforcement agency. A law
7 enforcement agency may request the delay if it believes that notification may
8 impede a law enforcement investigation or a national or Homeland Security
9 investigation or jeopardize public safety or national or Homeland Security
10 interests. In the event law enforcement makes the request for a delay in a
11 manner other than in writing, the data broker shall document the request
12 contemporaneously in writing and include the name of the law enforcement
13 officer making the request and the officer's law enforcement agency engaged
14 in the investigation. A law enforcement agency shall promptly notify the data
15 broker in writing when the law enforcement agency no longer believes that
16 notification may impede a law enforcement investigation or a national or
17 Homeland Security investigation or jeopardize public safety or national or
18 Homeland Security interests. The data broker shall provide notice required by
19 this subsection without unreasonable delay upon receipt of a written
20 communication, which includes facsimile or electronic communication, from
21 the law enforcement agency withdrawing its request for delay.

1 (4) The notice to a consumer required in subdivision (1) of this
2 subsection shall be clear and conspicuous. A notice to a consumer of a
3 security breach involving brokered personal information shall include a
4 description of each of the following, if known to the data broker:

5 (A) the incident in general terms;

6 (B) the categories of brokered personal information that was subject
7 to the security breach;

8 (C) the general acts of the data broker to protect the brokered
9 personal information from further security breach;

10 (D) a telephone number, toll-free if available, that the consumer may
11 call for further information and assistance;

12 (E) advice that directs the consumer to remain vigilant by reviewing
13 account statements and monitoring free credit reports; and

14 (F) the approximate date of the data broker security breach.

15 (5) A data broker may provide notice of a security breach involving
16 brokered personal information to a consumer by two or more of the following
17 methods:

18 (A) written notice mailed to the consumer's residence;

19 (B) electronic notice, for those consumers for whom the data broker
20 has a valid email address, if:

1 (i) the data broker’s primary method of communication with the
2 consumer is by electronic means, the electronic notice does not request or
3 contain a hypertext link to a request that the consumer provide personal
4 information, and the electronic notice conspicuously warns consumers not to
5 provide personal information in response to electronic communications
6 regarding security breaches; or

7 (ii) the notice is consistent with the provisions regarding electronic
8 records and signatures for notices in 15 U.S.C. § 7001;

9 (C) telephonic notice, for those consumers for whom the data broker
10 has a valid phone number, provided that the telephonic contact is made directly
11 with each affected consumer and not through a prerecorded message and
12 further provided that the data broker makes not less than five attempts to
13 contact the consumer for a live conversation before the data broker may leave a
14 voicemail providing information about the breach; or

15 (D) notice by publication in a newspaper of statewide circulation in
16 the event the data broker cannot effectuate notice by any other means.

17 (c) Exception to notice requirement.

18 (1) Notice of a security breach pursuant to subsection (b) of this section
19 is not required if the data broker establishes that misuse of brokered personal
20 information is not reasonably possible and the data broker provides notice of
21 the determination that the misuse of the brokered personal information is not

1 reasonably possible pursuant to the requirements of this subsection. If the data
2 broker establishes that misuse of the brokered personal information is not
3 reasonably possible, the data broker shall provide notice of its determination
4 that misuse of the brokered personal information is not reasonably possible and
5 a detailed explanation for said determination to the Attorney General. The data
6 broker may designate its notice and detailed explanation to the Attorney
7 General as a trade secret if the notice and detailed explanation meet the
8 definition of trade secret contained in 1 V.S.A. § 317(c)(9). Upon review of
9 the data broker's notice and detailed explanation, the Attorney General may
10 request additional information from the data broker and may accept or reject
11 the data broker's determination. If the Attorney General rejects the data
12 broker's determination, the data broker shall provide notice of the security
13 breach pursuant to subsection (b) of this section.

14 (2) If a data broker established that misuse of brokered personal
15 information was not reasonably possible under subdivision (1) of this
16 subsection and subsequently obtains facts indicating that misuse of the
17 brokered personal information has occurred or is occurring, the data broker
18 shall provide notice of the security breach pursuant to subsection (b) of this
19 section.

20 (d) Waiver. Any waiver of the provisions of this subchapter is contrary to
21 public policy and is void and unenforceable.

1 Subchapter 5. Data Brokers

2 § 2446. DATA BROKERS; ANNUAL REGISTRATION

3 (a) ~~Annually, on or before January 31 following a year in which a~~
4 Registration. A person meets, not more than 30 days after meeting the
5 definition of a data broker as provided in section 2430 of this title, a data
6 broker and then once annually thereafter on or before July 1 of each year, shall:

7 (1) register with the Secretary of State as a data broker;

8 (2) pay a registration fee of ~~\$100.00~~ \$900.00;

9 (3) maintain a bond in the amount of \$20,000.00 that shall run to the
10 State for any liability arising under this subchapter, provided that the action on
11 the bond is brought within two years after accrual of the cause of action; and

12 (4) provide the following information about the data broker to the
13 Secretary of State:

14 (A) the name and primary physical, ~~e-mail~~ email, phone number, and
15 Internet internet addresses of the data broker;

16 (B) ~~if the data broker permits a consumer to opt out of the data~~
17 ~~broker's collection of brokered personal information, opt out of its databases,~~
18 ~~or opt out of certain sales of data:~~

19 (i) ~~the method for requesting an opt out;~~

20 (ii) ~~if the opt out applies to only certain activities or sales, which~~
21 ~~ones; and~~

1 ~~(iii) whether the data broker permits a consumer to authorize a~~
2 ~~third party to perform the opt-out on the consumer's behalf;~~

3 ~~(C) a statement specifying the data collection, databases, or sales~~
4 ~~activities from which a consumer may not opt out;~~

5 ~~(D)~~ a statement whether the data broker implements a purchaser
6 credentialing process;

7 ~~(E)~~(C) pursuant to section 2436 of this chapter, the number of data
8 broker security breaches that the data broker has experienced during the prior
9 year, and if known, the total number of consumers affected by the breaches;

10 ~~(F)~~(D) where the data broker has actual knowledge that it possesses
11 the brokered personal information of minors, a separate statement detailing the
12 data collection practices, databases, sales activities, and opt-out policies that
13 are applicable to the brokered personal information of minors; ~~and~~

14 ~~(G)~~(E) whether the data broker:

15 (i) collects the:

16 (I) precise geolocation of consumers;

17 (II) reproductive health care data of consumers;

18 (III) biometric data of consumers;

19 (IV) immigration status of consumers;

20 (V) sexual orientation of consumers;

21 (VI) union membership status of consumers;

1 (VII) name, date of birth, zip code, email address, or phone
2 number of consumers;

3 (VIII) account login or account number of consumers in
4 combination with any required security code, access code, or password that
5 would permit access to a consumer's account with a third party;

6 (IX) driver's license number, State identification card number,
7 Social Security number, passport number, military identification number, or
8 other unique identification number of consumers issued on a government
9 document commonly used to verify the identity of a specific individual; or

10 (X) mobile advertising identification number, connected
11 television identification number, or vehicle identification number of
12 consumers; and

13 (ii) in the past year, has shared or sold consumers' data to:

14 (I) a foreign actor;

15 (II) the federal government;

16 (III) to other state or local governments;

17 (IV) to law enforcement, unless the data was shared pursuant to
18 a subpoena or other court order; or

19 (V) to a developer of a GenAI system or model;

1 (F) the three most common types of personal information that the
2 data broker collects, if the data broker does not collect the information set forth
3 in subdivisions (E)(i)(VII) and (E)(i)(IX) of this subdivision (4);

4 (G) an electronic copy of the data broker's:

5 (i) bond, pursuant to subdivision (3) of this subsection (a); and

6 (ii) current privacy policy;

7 (H) any additional information or explanation the data broker
8 chooses to provide concerning its data collection practices;

9 (I) the URL of a page on the data broker's website that:

10 (i) pursuant to subsection (c) of this section, allows a consumer to
11 request that a data broker delete the brokered personal information of the
12 consumer; and

13 (ii) informs consumers about the rights of consumers to opt out of
14 the collection of the consumer's brokered personal information, including:

15 (I) whether the data broker permits a consumer to opt out of its
16 databases, or opt out of certain sales of data;

17 (II) the procedure for requesting an opt-out;

18 (III) if the opt-out applies to only certain activities or sales,
19 which activities or sales it applies to;

20 (IV) whether the data broker permits a consumer to authorize
21 an authorized agent to perform the opt out on the consumer's behalf; and

1 (V) the data collection, databases, or sales activities from
2 which a consumer may not opt out; and

3 (J) whether and to what extent the data broker or any of its
4 subsidiaries is regulated by the Fair Credit Reporting Act; and

5 (5) amend an existing registration the data broker has with the Secretary
6 of State if required by this section or by the State upon the payment of an
7 administrative fee of \$100.00.

8 ~~(b) A data broker that fails to register pursuant to subsection (a) of this~~
9 ~~section is liable to the State for: Penalties.~~

10 ~~(1) a civil penalty of \$50.00 for each day, not to exceed a total of~~
11 ~~\$10,000.00 for each year, it fails to register pursuant to this section;~~

12 ~~(2) an amount equal to the fees due under this section during the period~~
13 ~~it failed to register pursuant to this section; and~~

14 ~~(3) other penalties imposed by law.~~

15 (1) A data broker that fails to register as required by subsection (a) of
16 this section is liable to the State for:

17 (A) an administrative fine of \$200.00 for each day the data broker
18 fails to register;

19 (B) an amount equal to the fees that were due during the period the
20 data broker failed to register; and

1 (C) any reasonable costs incurred by the State in the investigation
2 and administration of the action as the court deems appropriate.

3 (2) A data broker that fails to provide all registration information
4 required in subdivision (a)(4) of this section shall file an amendment pursuant
5 to subdivision (a)(5) of this section that includes any omitted information not
6 later than 30 days after discovering or receiving notification of the omission
7 and is liable to the State for a civil penalty of \$1,000.00 per day for each day
8 thereafter that the data broker does not file an amendment providing the
9 omitted information.

10 (3) A data broker that files materially incorrect information in its
11 registration shall:

12 (A) be liable to the State for a civil penalty of \$25,000.00; and

13 (B) correct the materially incorrect information by filing an
14 amendment pursuant to subdivision (a)(5) of this section not later than 30 days
15 after discovering or receiving notification of the incorrect information, and, if
16 it fails to correct the information, the data broker shall be liable for an
17 additional civil penalty of \$1,000.00 per day for each day the data broker fails
18 to correct the information.

19 ~~(c) The Attorney General may maintain an action in the Civil Division~~
20 ~~of the Superior Court to collect the penalties imposed in this section and to~~
21 ~~seek appropriate injunctive relief. Deleting brokered personal information.~~

1 (1) A data broker shall:

2 (A) maintain a conspicuous page on its website where a consumer or
3 an authorized agent of a consumer has the ability to request that the data broker
4 delete the consumer's brokered personal information free of charge;

5 (B) delete the consumer's brokered personal information not later
6 than 30 days after the consumer makes a deletion request pursuant to
7 subdivision (A) of this subdivision (1), unless the data broker denies the
8 request pursuant to subdivision (3) of this subsection (c); and

9 (C) notify the consumer that the consumer's brokered personal
10 information has been deleted not later than five days after the information has
11 been deleted.

12 (2) The web page maintained by a data broker pursuant to subdivision
13 (1) of this subsection shall:

14 (A) describe how a consumer may exercise the consumer's right to
15 delete the consumer's brokered personal information, including the process for
16 the consumer to appeal the denial of a deletion request pursuant to subdivision
17 (5) of this subsection (c);

18 (B) adhere to the accessibility and usability guidelines recommended
19 pursuant to 42 U.S.C. chapter 126 (the Americans with Disabilities Act) and
20 29 U.S.C. § 794d (section 508 of the Rehabilitation Act of 1973); and

1 (C) employ design practices that facilitate easy comprehension and
2 navigation for all users and that are free of any dark patterns.

3 (3) A data broker may deny a consumer's request to delete the
4 consumer's brokered personal information pursuant to subdivision (1) of this
5 subsection to the extent that:

6 (A) the retention of the consumer's brokered personal information is
7 required by law or is required to comply with a civil, criminal, or regulatory
8 inquiry, investigation, subpoena, or summons by a federal, state, municipal, or
9 other governmental authority; or

10 (B) the brokered personal information is:

11 (i) used by a consumer reporting agency to furnish a consumer
12 report pursuant to the Fair Credit Reporting Act;

13 (ii) necessary to investigate, establish, exercise, prepare for, or
14 defend a legal claim;

15 (iii) strictly necessary to fulfill a specific legal requirement on
16 behalf of a business to which the data broker is bound by a written contract to
17 fulfill that legal requirement;

18 (iv) used to prevent, detect, protect against, or respond to security
19 incidents, identity theft, fraud, harassment, or to preserve the technical
20 integrity or physical security of systems or investigate, report, or prosecute
21 those responsible for any such action;

- 1 (v) data that is collected or used for purposes of the National
2 Precursor Log Exchange, or its equivalent, pursuant to State or federal law;
3 (vi) processed solely in the data broker’s capacity as a processor to
4 a business with which the consumer has a direct relationship, as that term is
5 defined in subdivision 2430(a)(6)(B) of this chapter; or
6 (vii) used in connection with underwriting, issuing title insurance,
7 or completing an appraisal.
8 (4) Brokered personal information retained pursuant to subdivision (3)
9 of this subsection shall be:
10 (A) separated or segregated from data used for any other purpose;
11 (B) deleted immediately upon the expiration of the legal or
12 contractual requirement; and
13 (C) not used, sold, shared, or processed for any other purpose.
14 (5) A data broker shall provide the consumer with the ability to appeal
15 an instance where the data broker denies the consumer’s request to delete the
16 consumer’s brokered personal information pursuant to subdivision (3) of this
17 subsection (c) with a process that:
18 (A) gives the consumer 45 days after the consumer receives notice
19 that the data broker has denied the deletion request to initiate the appeal;

1 (B) is conspicuously available to the consumer;

2 (C) is similar to the manner in which a consumer submits a deletion
3 request pursuant to subdivision (1) of this subsection (c);

4 (D) requires the data broker to approve or deny the appeal within 45
5 days after the date on which the data broker received the appeal and to notify
6 the consumer in writing of the data broker’s decision and the reasons for the
7 decision; and

8 (E) requires a data broker that denies a consumer’s appeal to provide
9 information that enables the consumer to contact the Attorney General to
10 submit a complaint.

11 (6)(A) If a data broker is unable to authenticate a deletion request made
12 pursuant to subdivision (1) of this subsection (c), the data broker shall not be
13 required to comply with the request and shall provide notice to the consumer or
14 the consumer’s agent that the data broker is unable to authenticate the request.
15 The data broker shall provide the consumer with the additional information the
16 data broker requires in order to authenticate the consumer.

17 (B) As used in this subdivision (6), “authenticate” means the use of
18 reasonable measures to determine whether a deletion request is being made by,
19 or on behalf of, the consumer who is entitled to exercise that request with
20 respect to the brokered personal information at issue.

1 (d) Enforcement.

2 (1) A person who violates a provision of this section commits an unfair
3 and deceptive act in commerce in violation of section 2453 of this title.

4 (2) The Attorney General has the same authority to adopt rules to
5 implement the provisions of this ~~chapter~~ section and to conduct civil
6 investigations, enter into assurances of discontinuance, and bring civil actions
7 as provided under chapter 63, subchapter 1 of this title.

8 Sec. 2. STUDY OF ACCESSIBLE DELETION MECHANISM; REPORT;

9 APPROPRIATION

10 (a) The Secretary of State shall study the feasibility of:

11 (1) establishing an accessible deletion mechanism that:

12 (A) implements and maintains reasonable security procedures and
13 practices, including administrative, physical, and technical safeguards
14 appropriate to the nature of the information and the purposes for which
15 brokered personal information will be used and to protect a consumer's
16 brokered personal information from unauthorized use, disclosure, access,
17 destruction, or modification;

18 (B) allows a consumer, through a single verifiable consumer request,
19 to request that every data broker that maintains any brokered personal
20 information about the consumer delete the brokered personal information;

1 (C) allows a consumer to selectively exclude specific data brokers
2 from a request made under subdivision (B) of this subdivision (1);

3 (D) allows a consumer to alter a previous request made pursuant to
4 subdivision (B) of this subdivision (1) after at least 45 days have passed since
5 the consumer last made a request;

6 (E) allows a consumer to request the deletion of all brokered personal
7 information related to that consumer all at once through a single deletion
8 request;

9 (F) permits a consumer to securely submit information in one or
10 more privacy-protecting ways to aid in the deletion request;

11 (G) allows a data broker registered with the Secretary of State to
12 determine whether a consumer has submitted a verifiable request to delete the
13 brokered personal information related to that consumer as described in
14 subdivision (B) of this subdivision (1);

15 (H) does not allow the disclosure of any additional brokered personal
16 information of a consumer when the data broker accesses the accessible
17 deletion mechanism, unless otherwise specified in this subchapter;

18 (I) allows a consumer to make a request described in subdivision (B)
19 of this subdivision (1) using a website operated by the Secretary of State;

20 (J) does not charge a consumer to make a request described in
21 subdivision (B) of this subdivision (1);

1 (K) is readily accessible and usable by consumers with disabilities;

2 (L) supports the ability of a consumer's authorized agents to aid in
3 the deletion request;

4 (M) allows the consumer or their authorized agent to verify the status
5 of the consumer's deletion request; and

6 (N) provides a description of the following:

7 (i) the deletion permitted by this section;

8 (ii) the process for submitting a deletion request pursuant to this
9 section; and

10 (iii) examples of the types of information that may be deleted; and

11 (2) utilizing a data broker's registry fund to hold monies received for
12 transactions pursuant to 9 V.S.A. § 2446 and to disburse for the purpose of
13 supporting and offsetting the costs of the accessible deletion mechanism set
14 forth in subdivision (1) of this subsection.

15 (b) Reporting. The Secretary of State shall, based on the study set forth in
16 subsection (a) of this section, submit to the House Committee on Commerce
17 and Economic Development and the Senate Committee on Economic
18 Development, Housing and General Affairs an interim report on or before
19 December 1, 2027, and a final report on or before December 1, 2028, including
20 its findings and any proposed legislation for the General Assembly's

1 consideration. The interim report shall provide the General Assembly with any
2 recommended actions to pursue in the 2028 legislative session.

3 (c) Appropriation. In fiscal year 2027, \$50,000.00 is appropriated from the
4 General Fund to the Secretary of State for the purpose of hiring a consultant
5 that will provide support to the Secretary in the study pursuant to subsection
6 (a) of this section.

7 Sec. 3. EFFECTIVE DATE

8 This act shall take effect on January 1, 2027.