

1
2
3
4
5
6
7
8
9
10
11
12

13
14
15
16
17
18
19
20

S.70

Introduced by Senators Clarkson, Harrison, Hashim, Major, Vyhovsky and
White

Referred to Committee on

Date:

Subject: Commerce and trade; protection of personal information; data brokers

Statement of purpose of bill as introduced: This bill proposes to add various provisions to Vermont’s laws that protect the personal information of its residents, including requiring data brokers to provide notice of security breaches, to certify that the personal information it discloses will be used for a legitimate purpose, and to delete the personal information of consumers who make such a request through the use of an accessible deletion mechanism.

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:

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

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

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

7 (2)(A) “Biometric data” means data generated from the technological
8 processing of an individual’s unique biological, physical, or physiological
9 characteristics that is linked or reasonably linkable to an individual, including:

10 (i) iris or retina scans;

11 (ii) fingerprints;

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

13 (iv) vein patterns;

14 (v) voice prints; and

15 (vi) gait or personally identifying physical movement or patterns.

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

17 (i) a digital or physical photograph;

18 (ii) an audio or video recording; or

19 (iii) any data generated from a digital or physical photograph, or
20 an audio or video recording, unless such data is generated to identify a specific
21 individual.

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

4 (i) name;

5 (ii) address;

6 (iii) date of birth;

7 (iv) place of birth;

8 (v) mother’s maiden name;

9 (vi) ~~unique biometric data generated from measurements or~~
10 ~~technical analysis of human body characteristics used by the owner or licensee~~
11 ~~of the data to identify or authenticate the consumer, such as a fingerprint, retina~~
12 ~~or iris image, or other unique physical representation or digital representation~~
13 ~~of biometric data;~~

14 (vii) name or address of a member of the consumer’s immediate
15 family or household;

16 (viii) Social Security number or other government-issued
17 identification number; ~~or~~

18 (ix) phone number; or

19 (x) other information that, alone or in combination with the other
20 information sold or licensed, would allow a reasonable person to identify the
21 consumer with reasonable certainty.

1 (B) “Brokered personal information” does not include publicly
2 available information to the extent that it is related to a consumer’s business or
3 profession.

4 ~~(2)~~(4) “Business” means a controller, a consumer health data controller,
5 a processor, or a commercial entity, including a sole proprietorship,
6 partnership, corporation, association, limited liability company, or other group,
7 however organized and whether or not organized to operate at a profit,
8 including a financial institution organized, chartered, or holding a license or
9 authorization certificate under the laws of this State, any other state, the United
10 States, or any other country, or the parent, affiliate, or subsidiary of a financial
11 institution, but does not include the State, a State agency, any political
12 subdivision of the State, or a vendor acting solely on behalf of, and at the
13 direction of, the State.

14 ~~(3)~~(5) “Consumer” means an individual residing in this State.

15 (6) “Consumer health data controller” means any controller that, alone
16 or jointly with others, determines the purpose and means of processing
17 consumer health data.

18 (7) “Controller” means a person who, alone or jointly with others,
19 determines the purpose and means of processing personal data.

20 ~~(4)~~(8)(A) “Data broker” means a business, or unit or units of a business,
21 separately or together, that knowingly collects and sells or licenses to third

1 parties the brokered personal information of a consumer with whom the
2 business does not have a direct relationship.

3 (B) Examples of a direct relationship with a business include if the
4 consumer is a past or present:

5 (i) customer, client, subscriber, user, or registered user of the
6 business's goods or services within the last five calendar years;

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

8 (iii) investor in the business; or

9 (iv) donor to the business.

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

13 (i) developing or maintaining third-party e-commerce or
14 application platforms;

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

18 (iii) providing publicly available information related to a
19 consumer's business or profession; or

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

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

20 ~~(8)~~(12) “License” means a grant of access to, or distribution of, data by
21 one person to another in exchange for consideration. A use of data for the sole

1 benefit of the data provider, where the data provider maintains control over the
2 use of the data, is not a license.

3 ~~(9)~~(13) “Login credentials” means a consumer’s user name or ~~e-mail~~
4 email address, in combination with a password or an answer to a security
5 question, that together permit access to an online account.

6 ~~(10)~~(14)(A) “Personally identifiable information” means a consumer’s
7 first name or first initial and last name in combination with one or more of the
8 following digital data elements, when the data elements are not encrypted,
9 redacted, or protected by another method that renders them unreadable or
10 unusable by unauthorized persons:

11 (i) a Social Security number;

12 (ii) a driver license or nondriver State identification card number,
13 individual taxpayer identification number, passport number, military
14 identification card number, or other identification number that originates from
15 a government identification document that is commonly used to verify identity
16 for a commercial transaction;

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

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

1 (v) ~~unique biometric data generated from measurements or~~
2 ~~technical analysis of human body characteristics used by the owner or licensee~~
3 ~~of the data to identify or authenticate the consumer, such as a fingerprint, retina~~
4 ~~or iris image, or other unique physical representation or digital representation~~
5 ~~of biometric data;~~

6 (vi) genetic information; and

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

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

11 (III) a health insurance policy number.

12 (B) “Personally identifiable information” does not mean publicly
13 available information that is lawfully made available to the general public from
14 federal, State, or local government records.

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

18 (16) “Processor” means a person who processes personal data on behalf
19 of a controller.

1 ~~(11)~~(17) “Record” means any material on which written, drawn, spoken,
2 visual, or electromagnetic information is recorded or preserved, regardless of
3 physical form or characteristics.

4 ~~(12)~~(18) “Redaction” means the rendering of data so that the data are
5 unreadable or are truncated so that ~~no~~ not more than the last four digits of the
6 identification number are accessible as part of the data.

7 ~~(13)~~(19)(A) “Security breach” means unauthorized acquisition of
8 electronic data, or a reasonable belief of an unauthorized acquisition of
9 electronic data, that compromises the security, confidentiality, or integrity of a
10 consumer’s personally identifiable information or login credentials maintained
11 by a data collector.

12 (B) “Security breach” does not include good faith but unauthorized
13 acquisition of personally identifiable information or login credentials by an
14 employee or agent of the data collector for a legitimate purpose of the data
15 collector, provided that the personally identifiable information or login
16 credentials are not used for a purpose unrelated to the data collector’s business
17 or subject to further unauthorized disclosure.

18 (C) In determining whether personally identifiable information or
19 login credentials have been acquired or is reasonably believed to have been
20 acquired by a person without valid authorization, a data collector may consider
21 the following factors, among others:

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

4 (ii) indications that the information has been downloaded or
5 copied;

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

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

10 * * *

11 Subchapter 2. Security ~~Breach Notice Act~~ Breaches

12 § 2435. NOTICE OF SECURITY BREACHES

13 * * *

14 (h) Enforcement.

15 (1) ~~With respect to all data collectors and other entities subject to this~~
16 ~~subchapter, other than a person or entity licensed or registered with the~~
17 ~~Department of Financial Regulation under Title 8 or this title, the Attorney~~
18 ~~General and State's Attorney shall have sole and full authority to investigate~~
19 ~~potential violations of this subchapter and to enforce, prosecute, obtain, and~~
20 ~~impose remedies for a violation of this subchapter or any rules or regulations~~
21 ~~made pursuant to this subchapter as the Attorney General and State's Attorney~~

1 ~~have under chapter 63 of this title.~~ With respect to a controller or processor
2 other than a controller or processor licensed or registered with the Department
3 of Financial Regulation under Title 8 or this title, the Attorney General has the
4 same authority to adopt rules to implement the provisions of this section and to
5 conduct civil investigations, enter into assurances of discontinuance, bring civil
6 actions, and take other enforcement actions as provided under chapter 63,
7 subchapter 1 of this title. The Attorney General may refer the matter to the
8 State's Attorney in an appropriate case. The Superior Courts shall have
9 jurisdiction over any enforcement matter brought by the Attorney General or a
10 State's Attorney under this subsection.

11 (2) ~~With respect to a data collector that is a person or entity licensed or~~
12 ~~registered with the Department of Financial Regulation under Title 8 or this~~
13 ~~title, the Department of Financial Regulation shall have the full authority to~~
14 ~~investigate potential violations of this subchapter and to prosecute, obtain, and~~
15 ~~impose remedies for a violation of this subchapter or any rules or regulations~~
16 ~~adopted pursuant to this subchapter, as the Department has under Title 8 or this~~
17 ~~title or any other applicable law or regulation.~~ With respect to a controller or
18 processor that is licensed or registered with the Department of Financial
19 Regulation under Title 8 or this title, the Department of Financial Regulation
20 has the same authority to adopt rules to implement the provisions of this
21 section and to conduct civil investigations, enter into assurances of

1 discontinuance, bring civil actions, and take other enforcement actions as
2 provided under Title 8 or this title or any other applicable law or regulation.

3 * * *

4 § 2436. NOTICE OF DATA BROKER SECURITY BREACHES

5 (a) Short title. This section shall be known as the “Data Broker Security
6 Breach Notice Act.”

7 (b) Notice of breach to consumers.

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

18 (2) A data broker shall provide notice of a breach to the Attorney
19 General as follows:

20 (A)(i) The data broker shall notify the Attorney General of the date of
21 the security breach and the date of discovery of the breach and shall provide a

1 preliminary description of the breach within 14 business days, consistent with
2 the legitimate needs of the law enforcement agency, as provided in
3 subdivisions (3) and (4) of this subsection (b), after the data broker's discovery
4 of the security breach.

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

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

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

19 (ii) The data broker may send to the Attorney General a second
20 copy of the consumer notice, from which is redacted the type of brokered

1 personal information that was subject to the breach, that the Attorney General
2 shall use for any public disclosure of the breach.

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

20 (4) The notice to a consumer required in subdivision (1) of this
21 subsection shall be clear and conspicuous. A notice to a consumer of a

1 security breach involving brokered personal information shall include a
2 description of each of the following, if known to the data broker:

3 (A) the incident in general terms;

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

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

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

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

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

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

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

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

19 (i) the data broker's primary method of communication with the
20 consumer is by electronic means, the electronic notice does not request or
21 contain a hypertext link to a request that the consumer provide personal

1 information, and the electronic notice conspicuously warns consumers not to
2 provide personal information in response to electronic communications
3 regarding security breaches; or

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

6 (C) telephonic notice, provided that telephonic contact is made
7 directly with each affected consumer and not through a prerecorded message;
8 or

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

11 (c) Exception.

12 (1) Notice of a security breach pursuant to subsection (b) of this section
13 is not required if the data broker establishes that misuse of brokered personal
14 information is not reasonably possible and the data broker provides notice of
15 the determination that the misuse of the brokered personal information is not
16 reasonably possible pursuant to the requirements of this subsection. If the data
17 broker establishes that misuse of the brokered personal information is not
18 reasonably possible, the data broker shall provide notice of its determination
19 that misuse of the brokered personal information is not reasonably possible and
20 a detailed explanation for said determination to the Attorney General. The data
21 broker may designate its notice and detailed explanation to the Attorney

1 General as a trade secret if the notice and detailed explanation meet the
2 definition of trade secret contained in 1 V.S.A. § 317(c)(9).

3 (2) If a data broker established that misuse of brokered personal
4 information was not reasonably possible under subdivision (1) of this
5 subsection and subsequently obtains facts indicating that misuse of the
6 brokered personal information has occurred or is occurring, the data broker
7 shall provide notice of the security breach pursuant to subsection (b) of this
8 section.

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

11 (e) Enforcement.

12 (1) With respect to a controller or processor other than a controller or
13 processor licensed or registered with the Department of Financial Regulation
14 under Title 8 or this title, the Attorney General has the same authority to adopt
15 rules to implement the provisions of this section and to conduct civil
16 investigations, enter into assurances of discontinuance, bring civil actions, and
17 take other enforcement actions as provided under chapter 63, subchapter 1 of
18 this title. The Attorney General may refer the matter to the State's Attorney in
19 an appropriate case. The Superior Courts shall have jurisdiction over any
20 enforcement matter brought by the Attorney General or a State's Attorney
21 under this subsection.

1 (B) be deposited by the Secretary of State into the Data Brokers
2 Registry Fund established in section 2446b of this title; and

3 (3) provide the following information to the Secretary of State:

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

6 (B) if the data broker permits a consumer to opt out of the data
7 broker's collection of brokered personal information, opt out of its databases,
8 or opt out of certain sales of data:

9 (i) the method for requesting an opt-out;

10 (ii) if the opt-out applies to only certain activities or sales, which
11 ones; and

12 (iii) whether the data broker permits a consumer to authorize a
13 ~~third party~~ an authorized agent to perform the opt-out on the consumer's
14 behalf;

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

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

19 (E) the number of data broker security breaches that the data broker
20 has experienced during the prior year, and if known, the total number of
21 consumers affected by the breaches;

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

5 (G) whether the data broker collects:

6 (i) precise geolocation of consumers;

7 (ii) reproductive health care data of consumers;

8 (iii) Social Security numbers of consumers;

9 (iv) driver's license information of consumers;

10 (v) biometric data of consumers;

11 (vi) immigration status of consumers;

12 (vii) sexual orientation of consumers; or

13 (viii) union membership status of consumers;

14 (H) beginning on January 1, 2031, whether the data broker has
15 undergone an audit pursuant to subsection 2446a(d) of this title and if so, the
16 most recent year that the data broker has submitted a report resulting from the
17 audit to the Secretary of State;

18 (I) beginning on January 1, 2029, the following annual metrics
19 pursuant to section 2446a of this title:

20 (i) the number of deletion requests received;

21 (ii) the number of deletion requests processed;

1 (iii) the number of deletion requests denied because the consumer
2 request cannot be verified; and

3 (iv) the number of deletion requests denied because retention of
4 the consumer's brokered personal information is required by law; and

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

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

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

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

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

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

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

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

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

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

7 (3) A data broker that files materially incorrect information in its
8 registration:

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

10 (B) shall correct the incorrect information not later than 30 days after
11 notification of the incorrect information, and, if it fails to correct the
12 information, the data broker shall be liable for an additional civil penalty of
13 \$1,000.00 per day for each day the data broker fails to correct the information.

14 (4) All penalties, fines, fees, and expenses recovered in an action
15 pursuant to this section shall be deposited in the Data Brokers Registry Fund.

16 (c) Enforcement. The Attorney General and the Secretary of State may
17 maintain an action in the Civil Division of the Superior Court to collect the
18 penalties imposed in this section and to seek appropriate injunctive relief.

19 (d) Public web page. The Secretary of State shall create a publicly
20 accessible page on its website where it lists the registration information

1 provided by data brokers pursuant to this section and the accessible deletion
2 mechanism set forth in section 2446a of this title.

3 § 2446a. ACCESSIBLE DELETION MECHANISM

4 (a) Creation of mechanism. On or before January 1, 2028, the Secretary of
5 State shall establish an accessible deletion mechanism that:

6 (1) implements and maintains reasonable security procedures and
7 practices, including administrative, physical, and technical safeguards
8 appropriate to the nature of the information and the purposes for which the
9 brokered personal information will be used and to protect a consumer's
10 brokered personal information from unauthorized use, disclosure, access,
11 destruction, or modification;

12 (2) allows a consumer, through a single verifiable consumer request, to
13 request that every data broker that maintains any brokered personal
14 information about the consumer delete the brokered personal information;

15 (3) allows a consumer to selectively exclude specific data brokers from
16 a request made under subdivision (2) of this subsection;

17 (4) allows a consumer to alter a previous request made pursuant to
18 subdivision (2) of this subsection after at least 45 days have passed since the
19 consumer last made a request;

1 (5) allows a consumer to request the deletion of all brokered personal
2 information related to that consumer all at once through a single deletion
3 request;

4 (6) permits a consumer to securely submit information in one or more
5 privacy-protecting ways, as determined by the Secretary of State, to aid in the
6 deletion request;

7 (7) allows a data broker registered with the Secretary of State to
8 determine whether a consumer has submitted a verifiable request to delete the
9 brokered personal information related to that consumer as described in
10 subdivision (2) of this subsection;

11 (8) does not allow the disclosure of any additional brokered personal
12 information of a consumer when the data broker accesses the accessible
13 deletion mechanism, unless otherwise specified in this subchapter;

14 (9) allows a consumer to make a request described in subdivision (2) of
15 this subsection using a website operated by the Secretary of State;

16 (10) does not charge a consumer to make a request described in
17 subdivision (2) of this subsection;

18 (11) is readily accessible and usable by consumers with disabilities;

19 (12) supports the ability of a consumer's authorized agents to aid in the
20 deletion request;

1 (13) allows the consumer or their authorized agent to verify the status of
2 the consumer's deletion request; and

3 (14) provides a description of the following:

4 (A) the deletion permitted by this section;

5 (B) the process for submitting a deletion request pursuant to this
6 section; and

7 (C) examples of the types of information that may be deleted.

8 (b) Data broker access.

9 (1) Beginning on August 1, 2028, a data broker shall access the
10 accessible deletion mechanism established in subsection (a) of this section at
11 least once every 45 days and shall:

12 (A) process all verifiable deletion requests the data broker has
13 received from consumers in the previous 45 days and delete such brokered
14 personal information;

15 (B) process a request as an opt-out of the sale or sharing of the
16 consumer's brokered personal information;

17 (C) direct all service providers and contractors associated with the
18 data broker to:

19 (i) delete all brokered personal information related to a consumer
20 who has made a verifiable deletion request; and

1 (ii) process a request as an opt-out of the sale or sharing of the
2 consumer's brokered personal information; and

3 (D) not use or disclose any information submitted by a consumer
4 through the accessible deletion mechanism for any other purpose besides the
5 authority provided in this subsection (b), including for marketing purposes.

6 (2) A data broker may deny a consumer's request to delete a consumer's
7 brokered personal information made pursuant to this section if retention of the
8 consumer's brokered personal information is required by law.

9 (3) The Secretary of State may charge an access fee to a data broker to
10 use the accessible deletion mechanism that does not exceed the reasonable
11 costs of providing access.

12 (4) Any fees collected pursuant to subdivision (3) of this subsection
13 shall be deposited into the Data Brokers Registry Fund.

14 (c) Continuing obligation to consumers. Beginning on August 1, 2028,
15 once a data broker has processed a verifiable consumer request to delete a
16 consumer's brokered personal information, the data broker shall:

17 (1) delete all brokered personal information of the consumer at least
18 once every 45 days unless:

19 (A) the consumer alters the consumer's decision pursuant to
20 subdivision (a)(4) of this section; or

1 (B) retention of the consumer’s brokered personal information is
2 required by law; and

3 (2) not sell or share new brokered personal information of the consumer
4 unless the consumer expressly requests otherwise in writing;

5 (d) Audits.

6 (1) A data broker shall undergo an audit by an independent third party to
7 determine compliance with this section at least once every three years, with the
8 first audit taking place on or before December 31, 2030.

9 (2) For an audit completed pursuant to subdivision (1) of this
10 subsection, the data broker shall submit the report resulting from the audit and
11 any related materials to the Secretary of State within five business days of a
12 written request from the Secretary of State.

13 (3) A data broker shall maintain all reports and materials resulting from
14 audits conducted pursuant to this subsection for at least six years.

15 (e) Rules. The Secretary of State may adopt rules to implement the
16 provisions of this subchapter, except it shall not be permitted to create a rule
17 that establishes a new fee that is not authorized in this section.

18 (f) Penalties.

19 (1) A data broker that fails to comply with the requirements of this
20 section is liable to the State for:

1 (A) an administrative fine of \$200.00 per day for each deletion
2 request the data broker fails to complete as required by subsection (b) of this
3 section; and

4 (B) reasonable expenses incurred by the State in the investigation and
5 administration of the action.

6 (2) All penalties, fines, fees, and expenses recovered in an action
7 pursuant to subdivision (1) of this subsection shall be deposited in the Data
8 Brokers Registry Fund.

9 § 2446b. DATA BROKERS REGISTRY FUND

10 There is established the Data Brokers Registry Fund within the State
11 Treasury. The Fund shall be administered by the Secretary of State. All
12 monies collected or received by the Secretary of State and the Attorney
13 General pursuant to this subchapter shall be deposited into the Fund and shall
14 be made available for expenditure by the Secretary of State upon appropriation
15 by the General Assembly to offset the following costs:

16 (1) the reasonable costs of establishing and maintaining the
17 informational website as set forth in subsection 2446(d) of this title;

18 (2) the costs incurred by State courts and the Secretary of State in
19 connection with enforcing this subchapter; and

1 (3) the reasonable costs of establishing, maintaining, and providing
2 access to the accessible deletion mechanism described in section 2446a of this
3 title.

4 § 2446c. CREDENTIALING

5 (a) A data broker shall maintain reasonable procedures designed to ensure
6 that the brokered personal information it discloses is used for a legitimate and
7 legal purpose.

8 (b) These procedures shall require that prospective users of the brokered
9 information identify themselves, certify the purposes for which the information
10 is sought, and certify that the information shall be used for no other purpose.

11 (c) A data broker shall make a reasonable effort to verify the identity of a
12 new prospective user and the uses certified by the prospective user prior to
13 furnishing the user brokered personal information.

14 (d) A data broker shall not furnish brokered personal information to any
15 person if it has reasonable grounds for believing that the brokered personal
16 information will not be used for a legitimate and legal purpose.

17 § 2447. DATA BROKER DUTY TO PROTECT INFORMATION;

18 STANDARDS; TECHNICAL REQUIREMENTS

19 * * *

20 Sec. 2. EFFECTIVE DATE

21 This act shall take effect on July 1, 2025.