

1 TO THE HOUSE OF REPRESENTATIVES:

2 The Committee on Commerce and Economic Development to which was
3 referred House Bill No. 211 entitled “An act relating to data brokers and
4 personal information” respectfully reports that it has considered the same and
5 recommends that the bill be amended by striking out all after the enacting
6 clause and inserting in lieu thereof the following:

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

8 CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

9 Subchapter 1. General Provisions

10 § 2430. DEFINITIONS

11 As used in this chapter:

12 (1) “Authorized agent” means:

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

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

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

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

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

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

16 (i) name;

17 (ii) address;

18 (iii) date of birth;

19 (iv) place of birth;

20 (v) mother's maiden name;

1 (vi) 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 (vii) name or address of a member of the consumer's immediate
7 family or household;

8 (viii) Social Security number or other government issued
9 identification number; or

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

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

20 ~~(2)(4)~~ “Business” means a commercial entity, including a sole
21 proprietorship, partnership, corporation, association, limited liability company,

1 or other group, however organized and whether or not organized to operate at a
2 profit, including a financial institution organized, chartered, or holding a
3 license or authorization certificate under the laws of this State, any other state,
4 the United States, or any other country, or the parent, affiliate, or subsidiary of
5 a financial institution, but does not include the State, a State agency, any
6 political subdivision of the State, or a vendor acting solely on behalf of, and at
7 the direction of, the State.

8 ~~(3)(5)~~ “Consumer” means an individual residing in this State.

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

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

15 ~~(i) customer, client, subscriber, user, or registered user of the~~
16 ~~business's goods or services;~~

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

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

19 ~~(iv) donor to the business~~

20 As used in this subdivision (6), “direct relationship” means that a
21 consumer has intentionally interacted with a business for the purpose of

1 accessing, purchasing, using, requesting, or obtaining information about the
2 business's products or services. A consumer does not have a direct
3 relationship with a business if the purpose of the consumer's engagement is to
4 exercise a consumer right or for the business to verify the consumer's identity.
5 A business does not have a direct relationship with a consumer simply because
6 the business collects brokered personal information directly from the
7 consumer; the consumer must intend to interact with the business. A business
8 is still a data broker and does not have a direct relationship with a consumer as
9 to the brokered personal information the business sells about the consumer that
10 it collected outside of a first-party interaction with the consumer.

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

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

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

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

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

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

20 (C) In determining whether brokered personal information has been
21 acquired or is reasonably believed to have been acquired by a person without

1 ~~valid authorization, a data broker may consider the following factors, among~~

2 ~~others:~~

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

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

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

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

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

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

1 (9) “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 (10) “Identified or identifiable individual” means an individual who can
5 be readily identified, directly or indirectly.

6 (8)(11) “License” means a grant of access to, or distribution of, data by
7 one person to another in exchange for consideration. A use of data for the sole
8 benefit of the data provider, where the data provider maintains control over the
9 use of the data, is not a license.

10 (9)(12) “Login credentials” means a consumer’s user name or e-mail
11 email address, in combination with a password or an answer to a security
12 question, that together permit access to an online account.

13 (10)(13)(A) “Personally identifiable information” means a consumer’s
14 first name or first initial and last name in combination with one or more of the
15 following digital data elements, when the data elements are not encrypted,
16 redacted, or protected by another method that renders them unreadable or
17 unusable by unauthorized persons:

18 (i) a Social Security number;
19 (ii) a driver license or nondriver State identification card number,
20 individual taxpayer identification number, passport number, military
21 identification card number, or other identification number that originates from

1 a government identification document that is commonly used to verify identity
2 for a commercial transaction;

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

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

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

13 (vi) genetic information; and

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

16 (II) a health care professional's medical diagnosis or treatment
17 of the consumer; or

18 (III) a health insurance policy number.

19 (B) "Personally identifiable information" does not ~~mean include~~
20 publicly available information ~~that is lawfully made available to the general~~
21 ~~public from federal, State, or local government records.~~

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

4 (15) “Processor” means a person who performs any operation or set of
5 operations, whether by manual or automated means, on brokered personal
6 information or on sets of brokered personal information, such as the collection,
7 use, storage, disclosure, analysis, deletion, or modification of brokered
8 personal information on behalf of a data broker.

9 (16)(A) “Publicly available information” means information that:
10 (i) is made available:
11 (I) through federal, state, or local government records; or
12 (II) to the general public from widely distributed media; or
13 (ii) a data broker has a reasonable basis to believe that the
14 consumer has lawfully made available to the general public.

15 (B) “Publicly available information” does not include:
16 (i) biometric data collected by a business about a consumer
17 without the consumer’s knowledge;
18 (ii) information that is collated and combined to create a consumer
19 profile that is made available to a user of a publicly available website either in
20 exchange for payment or free of charge;

- (iii) information that is made available for sale;
- (iv) an inference that is generated from the information described in subdivision (ii) or (iii) of this subdivision (16)(B);
- (v) any obscene visual depiction, as defined in 18 U.S.C. § 1460;
- (vi) brokered personal information that is created through the combination of brokered personal information with publicly available information;
- (vii) genetic data, unless otherwise made publicly available by the consumer to whom the information pertains;
- (viii) information provided by a consumer on a website or online service made available to all members of the public, for free or for a fee, where the consumer has maintained a reasonable expectation of privacy in the information, such as by restricting the information to a specific audience; or
- (ix) intimate images, authentic or computer-generated, known to be nonconsensual.

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

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

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

4 (B) “Sale” does not include:

5 (i) the disclosure of brokered personal information to a processor
6 that processes the brokered personal information on behalf of the data broker;
7 (ii) the disclosure of brokered personal information to a third party
8 for purposes of providing a product or service requested by the consumer;
9 (iii) the disclosure or transfer of brokered personal information to
10 an affiliate of the data broker;
11 (iv) the disclosure, with the consumer’s consent, of brokered
12 personal information where the consumer directs the data broker to disclose the
13 brokered personal information or intentionally uses the data broker to interact
14 with a third party;
15 (v) the disclosure of publicly available information;
16 (vi) the disclosure or transfer of brokered personal information to
17 a third party as an asset that is part of a merger, acquisition, bankruptcy, or
18 other transaction, or a proposed merger, acquisition, bankruptcy, or other
19 transaction, in which the third party assumes control of all or part of the data
20 broker’s assets.

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 or data broker.

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 or data broker for a legitimate purpose
9 of the data collector or data broker, provided that the personally identifiable
10 information or login credentials are not used for a purpose unrelated to the data
11 collector’s or data broker’s business or subject to further unauthorized
12 disclosure.

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

17 (i) indications that the information is in the physical possession
18 and control of a person without valid authorization, such as a lost or stolen
19 computer or other device containing information;
20 (ii) indications that the information has been downloaded or
21 copied;

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

(b) Data brokers.

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

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

4 (3) A data broker shall make a reasonable effort to verify the identity of
5 a new prospective user and the uses certified by the prospective user prior to
6 furnishing the user brokered personal information.

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

10 (c) Enforcement.

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

13 (2) The Attorney General has the same authority to adopt rules to
14 implement the provisions of this section and to conduct civil investigations,
15 enter into assurances of discontinuance, bring civil actions, and take other
16 enforcement actions as provided under chapter 63, subchapter 1 of this title.

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

18 § 2435. NOTICE OF SECURITY BREACHES

19 * * *

1 (h) Enforcement.

20 * * *

1 § 2436. NOTICE OF DATA BROKER SECURITY BREACHES

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

4 (b) Notice of breach.

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

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

17 (A)(i) The data broker shall notify the Attorney General of the date of
18 the security breach and the date of discovery of the breach and shall provide a
19 preliminary description of the breach within 14 business days, consistent with
20 the legitimate needs of the law enforcement agency, as provided in

1 subdivisions (3) and (4) of this subsection (b), after the data broker's discovery
2 of the security breach.

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

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

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

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

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

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

1 provide personal information in response to electronic communications
2 regarding security breaches; or
3 (ii) the notice is consistent with the provisions regarding electronic
4 records and signatures for notices in 15 U.S.C. § 7001;
5 (C) telephonic notice, provided that telephonic contact is made
6 directly with each affected consumer and not through a prerecorded message;
7 or
8 (D) notice by publication in a newspaper of statewide circulation in
9 the event the data broker cannot effectuate notice by any other means.
10 (c) Exception.
11 (1) Notice of a security breach pursuant to subsection (b) of this section
12 is not required if the data broker establishes that misuse of brokered personal
13 information is not reasonably possible and the data broker provides notice of
14 the determination that the misuse of the brokered personal information is not
15 reasonably possible pursuant to the requirements of this subsection. If the data
16 broker establishes that misuse of the brokered personal information is not
17 reasonably possible, the data broker shall provide notice of its determination
18 that misuse of the brokered personal information is not reasonably possible and
19 a detailed explanation for said determination to the Attorney General. The data
20 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 data broker other than a data broker licensed or
13 registered with the Department of Financial Regulation under Title 8 or this
14 title, the Attorney General has the same authority to adopt rules to implement
15 the provisions of this section and to conduct civil investigations, enter into
16 assurances of discontinuance, bring civil actions, and take other enforcement
17 actions as provided under chapter 63, subchapter 1 of this title. The Attorney
18 General may refer the matter to the State's Attorney in an appropriate case.
19 The Superior Courts shall have jurisdiction over any enforcement matter
20 brought by the Attorney General or a State's Attorney under this subsection.

* * *

Subchapter 5. Data Brokers

10 § 2446. DATA BROKERS; ANNUAL REGISTRATION

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

- (1) register with the Secretary of State as a data broker;
- (2) pay a registration fee of \$100.00 **\$900.00**;

17 (3) maintain a bond in the amount of \$20,000.00 that shall run to the

18 State for any liability arising under this subchapter, provided that the action on

19 the bond is brought within two years after accrual of the cause of action; and

20 (4) provide the following information about the data broker to the
21 Secretary of State:

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

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

6 (i) ~~the method for requesting an opt out;~~
7 (ii) ~~if the opt out applies to only certain activities or sales, which~~
8 ~~ones; and~~

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

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

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

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

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

10 (J) whether and to what extent the data broker or any of its
11 subsidiaries is regulated by the Fair Credit Reporting Act.

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

14 (1) a civil penalty of \$50.00 for each day, not to exceed a total of
15 \$10,000.00 for each year, it fails to register pursuant to this section;

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

18 (3) other penalties imposed by law.

19 (1) A data broker that fails to register

20 this section is liable to the State for:

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

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

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

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

13 (3) A data broker that files materially incorrect information in its
14 registration:

15 (A) is liable to the State for a civil penalty of \$25,000.00; and
16 (B) shall correct the materially incorrect information not later than 30
17 days after notification of the incorrect information, and, if it fails to correct the
18 information, the data broker shall be liable for an additional civil penalty of
19 \$1,000.00 per day for each day the data broker fails to correct the information.

1 (c) Right to delete information.

2 (1) A consumer has the right to have the consumer's brokered personal
3 information deleted by a data broker. A data broker shall maintain a link on its
4 website where a consumer can request that the data broker delete the
5 consumer's brokered personal information.

6 (2) A data broker may deny a consumer's request to delete the

7 consumer's brokered personal information pursuant to subdivision (1) of this
8 subsection to the extent that:

13 (B) the brokered personal information is:

14 (i) used by a consumer reporting agency to furnish a consumer
15 report pursuant to the Fair Credit Reporting Act:

1 (iv) used to prevent, detect, protect against, or respond to security
2 incidents, identity theft, fraud, harassment, or to preserve the technical
3 integrity or physical security of systems or investigate, report, or prosecute
4 those responsible for any such action.

7 (A) separated or segregated from data used for any other purpose;

8 (B) deleted immediately upon the expiration of the legal or

9 contractual requirement; and

10 (C) not used, sold, shared, or processed for any other purpose.

11 (d) Consumer rights web page. The Secretary of State shall create and
12 maintain a publicly accessible page on its website that provides consumers
13 with the following:

6 (e) Enforcement. The Attorney General and the Secretary of State may
7 maintain an action in the Civil Division of the Superior Court to collect the
8 penalties imposed in this section and to seek appropriate injunctive relief.

9 § 2447. DATA BROKER DUTY TO PROTECT INFORMATION;

10 STANDARDS; TECHNICAL REQUIREMENTS

11 * * *

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

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

14 (1) establishing an accessible deletion mechanism that:

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

1 (B) allows a consumer, through a single verifiable consumer request,
2 to request that every data broker that maintains any brokered personal
3 information about the consumer delete the brokered personal information;
4 (C) allows a consumer to selectively exclude specific data brokers
5 from a request made under subdivision (B) of this subdivision (1);
6 (D) allows a consumer to alter a previous request made pursuant to
7 subdivision (B) of this subdivision (1) after at least 45 days have passed since
8 the consumer last made a request;
9 (E) allows a consumer to request the deletion of all brokered personal
10 information related to that consumer all at once through a single deletion
11 request;
12 (F) permits a consumer to securely submit information in one or
13 more privacy-protecting ways to aid in the deletion request;
14 (G) allows a data broker registered with the Secretary of State to
15 determine whether a consumer has submitted a verifiable request to delete the
16 brokered personal information related to that consumer as described in
17 subdivision (B) of this subdivision (1);
18 (H) does not allow the disclosure of any additional brokered personal
19 information of a consumer when the data broker accesses the accessible
20 deletion mechanism, unless otherwise specified in this subchapter;

2 of this subdivision (1) using a website operated by the Secretary of State;

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

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

10 (N) provides a description of the following:

11 (i) the deletion permitted by this section;

14 (iii) examples of the types of information that may be deleted:

19 (b) Reporting. The Secretary of State shall, based on the study set forth in
20 subsection (a) of this section, submit to the House Committee on Commerce
21 and Economic Development and the Senate Committee on Economic

1 Development, Housing and General Affairs an interim report on or before
2 November 15, 2026, and a final report on or before December 1, 2027,
3 including its findings and any proposed legislation for the General Assembly's
4 consideration. The interim report shall provide the General Assembly with any
5 recommended actions to pursue in the 2027 legislative session.

6 Sec. 3. EFFECTIVE DATE

7 This act shall take effect on July 1, 2026.

8 (Committee vote: _____)

9

10

Representative _____

11

FOR THE COMMITTEE