Guidance on Vermont's Act 171 of 2018
Data Broker Regulation

9 V.S.A. §§ 2430, 2433, 2446 and 2447

Issued by the Vermont Office of the Attorney General
December 11, 2018

TABLE OF CONTENTS

I. Who does this regulation apply to? 1

II. What is a Data Broker? 1

A. Does the business handle the data of consumers with whom they do not have a direct relationship? 2

B. Does the business both collect and sell or license the data? 2

C. Is the data about consumers who are Vermont residents? 3

D. Is the data brokered personal information? 4

E. Activities that do not qualify a business as a data broker 6

III. What are the obligations of a data broker? 6

A. Why are Data Brokers required to Register? 6

B. How Do I Register as a Data Broker? 6

C. What information must be provided? 7

D. What are the penalties for failure to register? 9

E. What are the minimum data security standards? 10

IV. Prohibited Acquisition of Personal Information 11

V. Additional Questions 11

1. If a data broker is registered to do business in Vermont, must it still register in the Data Broker Registry? 11

2. If the courts of Vermont would not have jurisdiction over a data broker, must it still register? 12

3. Are Data Brokers required to allow consumers to opt out of their collection, storage, or sale or licensing of their personal data. 12

Appendix A: Data Broker Filing Form

Appendix B: 9 V.S.A. § 2446: Data broker annual registration

Appendix C: 9 V.S.A. § 2447: Data broker duty to protect information; standards; technical requirements

Appendix D: 9 V.S.A. § 2431: Acquisition of brokered personal information; prohibitions

Data Broker Regulation Guidance

The purpose of this guidance is to provide clarity to the new data broker regulations (Act 171 of 2018) that are effective on January 1, 2019 and are codified in 9 V.S.A. §§ 2430, 2433, 2446 and 2447. This guide is not legal advice. In all instances the particular facts of any situation or actor will determine whether or how the law applies. This guide is intended to assist members of the data broker industry affected by this new regulation to help them comply with the law.

If, after reading the Guidance, you still have questions or still do not know if your business is required to comply with the law, please call the Vermont AG's Office at 802-828-3171. We will work with you to help you understand the law. You can also email ago.datasecurity@vermont.gov.

I. Who does this regulation apply to?

The regulation has three main parts:

1. A requirement that Data Brokers register with the Vermont Secretary of State annually and provide certain information;[1]
2. A requirement that Data Brokers maintain certain minimum data security standards;[2] and
3. A prohibition on fraudulently acquiring certain types of data, or using such data to commit bad acts.[3]

The sections involving registering and data security apply to **Data Brokers**. The section involving fraudulent acquisition of data, or acquisition of data to commit bad acts, applies to everyone.

II. What is a Data Broker?

The definition of Data Broker can be found in 9 V.S.A. § 2430(4).[4]

[1] *See* Section III.A-D.

[2] *See* Section III.E

[3] *See* Section IV.

[4] Definition of "Data Broker":

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

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

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

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

(iii) investor in the business; or

(iv) donor to the business.

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

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

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

In determining whether a business is considered a data broker, ask these questions:

A. Does the business handle the data of consumers with whom they <u>do not have a direct relationship</u>?

Data brokers collect and sell or license the data of consumers with whom they do not have a direct relationship. This means that, for example:

1. a retailer that sells information about its customers is not a data broker
2. a charity that sells information about its donors is not a data broker
3. a business that sells information about its employees is not a data broker
4. an application, website, or social media platform that sells information about its users is not a data broker
5. a magazine that sells information about its subscribers is not a data broker
6. a realtor that sells information about her clients is not a data broker
7. a corporation that sells information about its investors is not a data broker

Examples in the statute of direct relationships include past or present customers, clients, subscribers, users, registered users, employees, contractors, agents, investors, and donors. This list is non-exclusive.

B. Does the business <u>both</u> <u>collect</u> and <u>sell or license</u> the data?

A business that collects data for its own use or analysis is not a data broker. So, for example:

1. An insurance company that buys data about individuals in order to set rates and develop new products, but does not resell the data, is not a data broker.
2. A business that acquires lists of individuals in order to market to them or customize their product offerings, but does not resell the data, is not a data broker.
3. A realtor that acquires information about potential customers in order to send out marketing mailings, but who does not resell the data, is not a data broker.
4. A news organization that collects data about individuals in order to produce news articles, is not a data broker.

Note that some businesses, like a newspaper, might acquire information in order to supply analysis or journalism. These businesses are not data brokers. However, a business that collects information about consumers and then adds additional data elements, cleans up the data, or

---

(iii) providing publicly available information related to a consumer's business or profession; or
(iv) providing publicly available information via real-time or near real-time alert services for health or safety purposes.

(D) The phrase "sells or licenses" does not include:
(i) a one-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business; or
(ii) a sale or license of data that is merely incidental to the business.

categorizes the data into lists in order to sell or license the data or a subset of the data to others, is a data broker.

Collection is a broad term. It can include the purchase or license of data from someone else, or collection from original sources like court records, other government records, surveys, or internet search histories.

Sale or **license** of data means supplying data to someone else in exchange for consideration. Consideration need not be monetary. It can include barter, in-kind exchanges, other data sets, or anything of value. If a company gives away a dataset, and receives nothing in return, then it has not sold or licensed the data. The distinction between the terms sale and license is that in a sale, ownership of the data set passes to the purchaser or the purchaser obtains the ability to do whatever it wants with the data and the seller releases all control. In a licensing agreement, the ownership of the dataset stays with the licensor, and the licensee has more limited control over what it can do with the data. For example, it may only have access to the data for a limited term.

If an owner of data supplies the data to a third party so that the third party can use the data for the sole benefit of the owner, this is not considered a license. For example:

1. A company providing a mailing list of non-customers to a printer in order to send out mailings on behalf of the provider is not licensing the data so long as the printer then destroys the data or does not use it for its own purposes.
2. A company providing data of non-customers to an analysis firm that will clean up, analyze, or supplement the data, and then return the data set to the provider, is not licensing the data, so long as the analysis firm is not permitted to continue to use the data for its own purposes or resell the data.
3. A financial firm providing a data set to an analysis firm in order to receive reports and market analysis is not licensing the data as long as the analysis firm will destroy the data when the analysis is completed or not use it for its own purposes.

"Sale or license" does not include a one-time or occasional sale of the assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business. It also doesn't include a sale or license that is "merely incidental to the business." If a business is unsure whether either of these exceptions applies to its sales or licensing of data, it should contact the Attorney General's office.

C. Is the data about consumers who are Vermont residents?

For purposes of the data broker regulations, **Consumer** is defined as an individual residing in the state of Vermont.[5]

That means that if you have no data of Vermont residents, Vermont's data broker regulation does not apply to you. It is the data broker's responsibility to determine whether or not it

[5] 9 V.S.A. § 2430(3)

possesses data of Vermonters. Although Vermont has a relatively small population, if you are a data broker with a national scope, there is a non-trivial chance you possess Vermonters' data, so if you do not maintain the state of residence of individuals whose data you collect, you might presume that there may be at least one Vermonter in your data set.

Please note that, as with any law, it is only applicable if the State of Vermont would be able to assert jurisdiction over your business.

D. Is the data brokered personal information?

Data brokers deal in "**brokered personal information**," which is a defined term in 9 V.S.A. § 2430(1).[6]

Brokered personal information (BPI) is a broad definition intended to cover a wide array of data, but it has limits. First, BPI must be computerized – information solely in paper form is not BPI.

Second, the information must be categorized or organized for dissemination to third parties. This means that the business that possesses the data must have done something to the data to prepare it for dissemination outside the business. For example, BPI includes data that has been categorized by characteristics of consumers (*i.e.* "People with incomes over $100,000," "People who like to play billiards," "People preparing for a wedding"). Data that is stored in a business's databases for the internal use by that business, with no intention of disseminating outside the business, is not BPI.

If the data contains one of the following elements, it is BPI:

1. name;
2. address;

[6] Definition of "Brokered personal information":

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

(i) name;
(ii) address;
(iii) date of birth;
(iv) place of birth;
(v) mother's maiden name;
(vi) unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;
(vii) name or address of a member of the consumer's immediate family or household;
(viii) Social Security number or other government-issued identification number; or
(ix) other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty.

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

3. date of birth;
4. place of birth;
5. mother's maiden name;
6. biometric information (as defined in fn 3);
7. name or address of a member of the consumer's immediate family or household;
8. Social Security number or other government-issued identification number.

Because data brokers may collect thousands of data elements about a consumer which do not appear on the above list, but which could allow the consumer to be identified, BPI also includes:

9. other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty.

As explained in the Data Broker Working Group Report, numerous studies have shown that data can easily be re-identified with an individual based on as few as three data elements. Data scientists have demonstrated the ability to re-identify consumers from "anonymized" datasets like customer transaction records, online movie viewing history, hospitalization records, and taxi ride records.

If a business is collecting and selling or licensing datasets that include information about individuals, even if the sets do not include the first eight elements listed above, it has a duty to determine whether or not its dataset is reasonably re-identifiable.

Finally, BPI does not include publicly available information only to the extent that it is related to a business or profession. For example, a doctor's office address or phone number is not BPI, but a doctor's home phone number (assuming it is not used for business) is BPI. The idea behind this exemption is that while people have a privacy interest in their personal information, they generally do not want to keep their business contact information private. The purpose of this exemption was to exclude entities that publish business directories, professional websites, politician contact lists, and other such collections of information that do not raise privacy concerns.

Note that while all data brokers deal in BPI, not all BPI is necessarily dealt in by data brokers. As described below, this regulation makes fraudulent acquisition of BPI illegal. That could be BPI acquired from any source, not just from data brokers. (The term brokered personal information was chosen to distinguish this definition from the numerous other definitions of Personally Identifiable Information (PII) and personal information found in other sections of the Vermont Statutes.)

If you answered "yes" to the previous four questions, and your business's activities don't fall within the following exceptions, your business is a data broker.

E. Activities that do not qualify a business as a data broker:

1. developing or maintaining third-party e-commerce or application platforms;
2. providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier;
3. providing publicly available information related to a consumer's business or profession; or
4. providing publicly available information via real-time or near real-time alert services for health or safety purposes.

Note that a business could be a data broker and also engage in the above activities. This exemption simply means that these activities, with nothing more, does not qualify a business as a data broker.

III. What are the obligations of a data broker?

The data broker regulation requires data brokers to do two things:

1. Register with the Vermont Secretary of State annually and provide certain information; and
2. Maintain certain minimum data security standards.

A. Why are Data Brokers required to Register?

The purpose of this requirement is to provide consumers with factual, non-controversial information to help consumers protect themselves and to avoid deception that could relate to data broker activities.

B. How Do I Register as a Data Broker?

Each year, any business that operated as a data broker during the prior year must register with the Vermont Secretary of State by filling out an online form located at https://www.vtsosonline.com/online.[7] The form will be available on January 1, 2019.

The deadline the annual filing is January 31 of each year, beginning in 2019.

The filing fee is $100.

Any business that operated as a Data Broker in 2018 is required to register by January 31, 2019.

[7] 9 V.S.A. § 2446

A copy of the filing form can be found in Appendix A to this guidance. You can also register by mail by sending a copy of the form to:

Vermont Secretary of State's Office
Corporations Division
128 State Street
Montpelier, VT 05633-1104

Each response should be answered with specificity. A reference to a company website, general policy or terms of service would not be an appropriate response. You may supplement your response with a reference to a specific page of a website, but this should not replace a specific response.

C. What information must be provided?

The form requires the following information be provided:

1. **A contact to whom acknowledgement that the information has been received can be provided;**
2. **The name and primary physical, e-mail, and internet addresses of the data broker;**
3. **If the data broker permits a consumer to opt out of the data broker's collection of brokered personal information, opt out of its databases, or opt out of certain sales of data:**
   a. **the method for requesting an opt-out;**
   b. **if the opt-out applies to only certain activities or sales, which ones; and**
   c. **whether the data broker permits a consumer to authorize a third party to perform the opt-out on the consumer's behalf;**
4. **A statement specifying the data collection, databases, or sales activities from which a consumer may not opt out;**

The regulation does not require a business to permit consumers to opt out of its collection, sales, or storage of their information, if that is not its practice. During hearings, however, industry representatives stated that providing opt-outs is a "best practice." If the data broker does permit opt-outs, it must describe how a consumer can do so.

If a business permits opt-outs from certain collection, sales, or storage but not from others, it must specify which ones the consumer can opt out of in response to question 3.b. It must specify which ones the consumer <u>cannot</u> opt out of in response to question 4. These questions must be answered with specificity.

It has been reported that some data brokers have policies that a consumer must personally request to be opted out, and may not authorize a relative, agent, business, or any other third-party to do so on their behalf. If the business does not permit such third-party opt outs it must state so.

5. **A statement whether the data broker implements a purchaser credentialing process;**

There have been instances of data brokers providing consumer data to scammers, identity thieves, and other criminals. "Credentialing" refers to the practice of taking reasonable steps to confirm that a data broker's customers are who they say they are, will be using the data collected for the purposes that they say they will be using it for, and will not use the data for nefarious purposes. During hearings industry representatives stated that having a credentialing process is a "best practice."

The regulation does not require a business to have a credentialing process, but it must state whether it does so.

6. **The number of data broker security breaches that the data broker has experienced during the prior year, and if known, the total number of consumers affected by the breaches;**

"Data Broker Security Breach" is defined in 9 V.S.A. § 2430(5).[8] The definition tracks the definition of "Security Breach" used in the Vermont Security Breach Notice Act.[9] However:

- whereas a "Security Breach" involves Personally Identifiable Information (PII) [10] maintained by a Data Collector,[11]
- a "Data Broker Security Breach" involves Brokered Personal Information[12] maintained by a Data Broker. [13]

[8] (5)(A) "Data broker security breach" means an unauthorized acquisition or a reasonable belief of an unauthorized acquisition of more than one element of brokered personal information maintained by a data broker when the brokered personal information is not encrypted, redacted, or protected by another method that renders the information unreadable or unusable by an unauthorized person.
(B) "Data broker security breach" does not include good faith but unauthorized acquisition of brokered personal information by an employee or agent of the data broker for a legitimate purpose of the data broker, provided that the brokered personal information is not used for a purpose unrelated to the data broker's business or subject to further unauthorized disclosure.
(C) In determining whether brokered personal information has been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data broker may consider the following factors, among others:
(i) indications that the brokered personal information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing brokered personal information;
(ii) indications that the brokered personal information has been downloaded or copied;
(iii) indications that the brokered personal information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or
(iv) that the brokered personal information has been made public.
[9] 9 V.S.A. § 2435.
[10] 9 V.S.A. § 2430(9).
[11] 9 V.S.A. § 2430(6).
[12] 9 V.S.A. § 2430(1).
[13] 9 V.S.A. § 2430(4).

Data Brokers generally are explained further in Section II above, and Brokered Personal Information is explained in Section II.D. Importantly, where a security breach may be experienced by any type of business, but only involves a small subset of data (social security numbers, credit card numbers, etc.), a Data Broker Security Breach may only be experienced by a data broker, but includes a broader set of data, and is not limited to PII.

Unlike in the Security Breach Notice Act, there is no duty to notify consumers or the Attorney General of a Data Broker Security Breach. However, Data Brokers must track the number of Data Broker Security Breaches they experience, and report that number annually as part of the annual registration, as well as the number of Vermont consumers affected by the breaches, if known.[14] Note: A statement provided pursuant to this reporting requirement does not absolve responsibility for providing notice to the State and consumer if PII is involved.

7. Where the data broker has actual knowledge that it possesses the brokered personal information of minors, a separate statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the brokered personal information of minors; and

A minor is any individual under the age of 18 years old. The "actual knowledge" requirement means that if a data broker does not have age information, it is not required to supplement its data in order to determine the ages of the consumers whose data it collects, maintains, or sells. However, if the data broker does have sufficient information to know that its data set contains minors, it must comply with this requirement.

8. Any additional information or explanation the data broker chooses to provide concerning its data collection practices.

This section is optional. All information provided to the registry will be available to the public. The data broker may choose to provide additional information to provide context for its practices, or choose to provide other information that it wants those viewing its statements to know.

D. What are the penalties for failure to register?

A data broker required to register that fails to do so will be subject to a penalty of $50 for each day it fails to register, beginning February 1, 2019, up to a maximum of $10,000 per year. The data broker will also be required to pay the $100 registration fee.

This is the same penalty applied to foreign corporations that fail to register to do business in Vermont.

[14] The statute uses the word "consumers," which is defined in 9 V.S.A. § 2430(3) as "an individual residing in this State."

E. What are the minimum data security standards?

All businesses are required to maintain reasonable data security. The failure to do so is considered an unfair or deceptive act under Vermont's Consumer Protection Act. While all businesses must protect the data entrusted to them, the risk of data breaches by data brokers is of particular concern because they collect large amounts of consumers' sensitive data, the acquisition of which can lead to identity theft, fraud, and spear-phishing attempts. The duty to protect information is set forth in 9 V.S.A. § 2447, and applies only to the handling of PII, not Brokered Personal Information. The complete text of this statute is included in Appendix C.

This duty tracks the language found in a Massachusetts regulation, 201 C.M.R. 17. Any business that collects PII and has a customer who is a Massachusetts resident is already required to comply with these standards.[15]

Although you should carefully read the full text of this statute in order to comply, some critical elements include requirements to implement the following business practices:

1. Develop, implement and maintain a comprehensive security program that is in writing;
2. Designate one or more employees to maintain the program;
3. Perform a risk assessment;
4. Train employees (including temporary and contract employees);
5. Track employee compliance with policy and procedures;
6. Have a means for detecting and preventing security system failures;
7. Have security policies for employees relating to storage, access, and transportation of PII outside business premises;
8. Have disciplinary measures for violations of the program rules;
9. Have measures that prevent terminated employees from accessing PII;
10. Supervise service providers;
11. Restrict physical access to PII;
12. Monitor the program and upgrade it as needed;
13. Review the scope of the security measures at least annually or whenever there is a material change in business practices that might impact security of PII;
14. Document responsive actions taken in connection with security breaches and review such incidents to determine whether practices should change.

The data broker, involving the sale or licensing of PII, must also implement the following computer system requirements:

1. Secure user authentication protocols;
2. Secure access control measures;

[15] Vermont's standard deviates from the Massachusetts regulation in one respect: Vermont's standard provides businesses with the flexibility to provide certain protections other than those proscribed, so long as they provide a higher degree of security.

3. Encryption of transmitted records and files containing PII that will traverse public networks, and encryption of all data containing PII to be transmitted wirelessly;
4. Monitoring of systems for unauthorized use or access to PII;
5. Encryption of PII on laptops or portable devices;
6. Firewalls and operating system patches;
7. Up-to-date malware, patching, and virus definitions; and
8. Training of employees on proper use of computer security and the importance of personal information security.

IV. Prohibited Acquisition of Personal Information[16]

It is now illegal to:

1. Acquire brokered personal information through fraudulent means; and
2. Acquire brokered personal information for the purpose of:
    a. Stalking or harassing someone;
    b. Committing fraud, including identity theft, financial fraud, or e-mail fraud; or
    c. Engaging in unlawful discrimination, including employment discrimination and housing discrimination.

This prohibition applies to all businesses and individuals, not just data brokers. The relevant statute uses the same personal information definition ("Brokered Personal Information") used in the data broker sections. "Brokered Personal Information" does not mean information acquired from or sold by a data broker. Brokered Personal Information is further explained in Section II.D.

The concepts of fraud, stalking and harassing, identity theft, and unlawful discrimination are addressed in the common law and other statutes.

Violation of this law is considered a violation of the Consumer Protection Act. This means that an action could be brought by the Attorney General for penalties of up to $10,000 per violation in addition to other relief. A consumer may bring an action for injunctive relief, damages, and attorneys' fees. There are no criminal penalties associated with violation of this law, aside from engaging in an associated criminal act.

V. Additional Questions

1. If a data broker is registered to do business in Vermont, must it still register in the Data Broker Registry?

Yes, the Data Broker Registry and the Corporations Registry serve different purposes.

[16] 9 V.S.A. § 2433.

2. **If the courts of Vermont would not have jurisdiction over a data broker, must it still register?**

No. Like all state laws, this law only applies to businesses over which Vermont courts could assert jurisdiction. This law is not an attempt to regulate businesses throughout the United States, only those that could be subject to jurisdiction in Vermont.

That said, if in the interest of transparency a data broker not otherwise subject to Vermont jurisdiction wishes to register in Vermont, it may do so.

3. **Are Data Brokers required to allow consumers to opt out of their collection, storage, or sale or licensing of their personal data?**

No. There is no requirement to change any business practice other than reporting annually, maintaining a comprehensive data security program consistent with that required elsewhere, and tracking Data Broker Data Breaches so that data brokers can report them annually.

Appendix A

Data Broker Filing Form

Vermont Secretary of State

ANNUAL REGISTRATION OF DATA BROKERS

"Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship. 9 V.S.A. § 2430(4).

Registration ID: _____

1. Return Acknowledgement to: Required - Name and Address

Name

Address

Address

Address

Processed by: _____
FOR OFFICE USE ONLY

This registration is required annually between January 1 and January 31 following a calendar year in which a person meets the definition of a data broker as provided above. 9 V.S.A. § 2446.

Each response should be answered with specificity. A reference to a company website, general policy or terms of service would not be an appropriate response. You may supplement your response with a reference to a specific page of a website, but this may not replace a specific response.

2. Data Broker[1] Information. Required.

a. Name: _____

b. Primary Physical Address: _____

c. Primary Email Address: _____

d. Primary Internet Address (URL): _____

3. Does the data broker permits a consumer to opt out of the data broker's collection of brokered personal information,[2] opt out of its databases, or opt out of certain sales of data? Required. ☐ **Yes** ☐ **No**

If so:

a. What is the method for requesting an opt-out?

b. If the opt-out applies to only certain activities or sales, which ones?

c. Does the data broker permits a consumer to authorize a third party to perform the opt-out on the consumer's behalf?

4. Statement specifying the data collection, databases, or sales activities from which a consumer may not opt out: Required.

5. Statement regarding whether the data broker implements a purchaser credentialing process: Required.

6. Statement regarding whether the data broker implements a purchaser credentialing process: Required.

Vermont Secretary of State
ANNUAL REGISTRATION
of Data Brokers

7. a. The number of security breaches[3] that the data broker[1] has experienced during the prior year: Required._____.

b. If known, the total number of Vermont residents affected by the breaches: _____.

8. Where the data broker has actual knowledge that it possesses the brokered personal information[2] of minors, a statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the brokered personal information of minors: Required.

9. Any additional information or explanation the data broker chooses to provide concerning its data collection practices: Optional.

10. Certification of Annual Registration: Required.

I hereby certify, under penalty of law (13 V.S.A. Ch. 65), as an authorized representative of the data broker, that the all of the above information is accurate; and that this document is provided with a Check or Money Order, payable to "VT SOS" in the amount of **$100.00**.

Printed Name	Signature	Date

[1] "Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship. Examples of a direct relationship with a business include if the consumer is a past or present customer, client, subscriber, user, or registered user of the business's goods or services; employee, contractor, or agent of the business; investor in the business; or donor to the business. The following activities conducted by a business, and the collection and sale or licensing of brokered personal information incidental to conducting these activities, do not qualify the business as a data broker: developing or maintaining third-party e-commerce or application platforms; providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier; providing publicly available information related to a consumer's business or profession; or providing publicly available information via real-time or near-real-time alert services for health or safety purposes. The phrase "sells or licenses" does not include: a one-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business; or a sale or license of data that is merely incidental to the business. 9 V.S.A. § 2430(4).

[2] "Brokered personal information" means one or more of the following computerized data elements about a consumer, if categorized or organized for dissemination to third parties: name; address; date of birth; place of birth; mother's maiden name; unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data; name or address of a member of the consumer's immediate family or household; Social Security number or other government-issued identification number; or other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty. "Brokered personal information" does not include publicly available information to the extent that it is related to a consumer's business or profession. 9 V.S.A. § 2430(1).

[3] "Security breach" means unauthorized acquisition of, electronic data or a reasonable belief of an unauthorized acquisition of, electronic data that compromises the security, confidentiality or integrity of a consumer's personally identifiable information maintained by a data collector. "Security breach" does not include good faith but unauthorized acquisition of personally identifiable information by an employee or agent of the data collector for a legitimate purpose of the data collector; provided that the personally identifiable information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure. In determining whether personally identifiable information has been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data collector may consider the following factors, among others: indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information; indications that the information has been downloaded or copied; indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or that the information has been made public. 9 V.S.A. § 2430(12).

Vermont Secretary of State
ANNUAL REGISTRATION OF DATA BROKERS

Submission Instructions

a. *This form* must be submitted with a check or money order, payable to "VT SOS," in the amount of $100.00, and a self-addressed stamped envelope.

b. *This form* can **ONLY** be accepted by Mail or In-person at:

Vermont Secretary of State
Corporations Division
128 State Street
Montpelier, VT 05633-1104

c. Please allow 7-10 business days, or more, from the day that *this form* is received in our office, for processing and (if approved) for this business to appear on the website at www.vtsosonline.com, and for evidence of filing to be returned.

Appendix B

9 V.S.A. § 2446:
Data broker annual registration

The Vermont Statutes Online
Title 9: Commerce And Trade
Chapter 062: Protection Of Personal Information
Subchapter 005: Data Brokers

(Cite as: 9 V.S.A. § 2446)

[Section 2446 effective January 1, 2019.]

§ 2446. Annual registration

(a) Annually, on or before January 31 following a year in which a person meets the definition of data broker as provided in section 2430 of this title, a data broker shall:

(1) register with the Secretary of State;

(2) pay a registration fee of $100.00; and

(3) provide the following information:

(A) the name and primary physical, e-mail, and Internet addresses of the data broker;

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

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

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

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

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

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

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

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

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

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

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

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

(3) other penalties imposed by law.

(c) The Attorney General may maintain an action in the Civil Division of the Superior Court to collect the penalties imposed in this section and to seek appropriate injunctive relief. (Added 2017, No. 171 (Adj. Sess.), § 2, eff. Jan. 1, 2019.)

Appendix C

9 V.S.A. § 2447:
Data broker duty to protect information; standards; technical requirements

The Vermont Statutes Online
Title 9: Commerce And Trade
Chapter 062: Protection Of Personal Information
Subchapter 005: Data Brokers

(Cite as: 9 V.S.A. § 2447)

[Section 2447 effective January 1, 2019.]

§ 2447. Data broker duty to protect information; standards; technical requirements

(a) Duty to protect personally identifiable information.

(1) A data broker shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to:

(A) the size, scope, and type of business of the data broker obligated to safeguard the personally identifiable information under such comprehensive information security program;

(B) the amount of resources available to the data broker;

(C) the amount of stored data; and

(D) the need for security and confidentiality of personally identifiable information.

(2) A data broker subject to this subsection shall adopt safeguards in the comprehensive security program that are consistent with the safeguards for protection of personally identifiable information and information of a similar character set forth in other State rules or federal regulations applicable to the data broker.

(b) Information security program; minimum features. A comprehensive information security program shall at minimum have the following features:

(1) designation of one or more employees to maintain the program;

(2) identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper, or other records containing personally identifiable information, and a process for evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including:

(A) ongoing employee training, including training for temporary and contract employees;

(B) employee compliance with policies and procedures; and

(C) means for detecting and preventing security system failures;

(3) security policies for employees relating to the storage, access, and transportation of records containing personally identifiable information outside business premises;

(4) disciplinary measures for violations of the comprehensive information security program rules;

(5) measures that prevent terminated employees from accessing records containing personally identifiable information;

(6) supervision of service providers, by:

(A) taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personally identifiable information consistent with applicable law; and

(B) requiring third-party service providers by contract to implement and maintain appropriate security measures for personally identifiable information;

(7) reasonable restrictions upon physical access to records containing personally identifiable information and storage of the records and data in locked facilities, storage areas, or containers;

(8)(A) regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personally identifiable information; and

(B) upgrading information safeguards as necessary to limit risks;

(9) regular review of the scope of the security measures:

(A) at least annually; or

(B) whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personally identifiable information; and

(10)(A) documentation of responsive actions taken in connection with any incident involving a breach of security; and

(B) mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personally identifiable information.

(c) Information security program; computer system security requirements. A comprehensive information security program required by this section shall at minimum, and to the extent technically feasible, have the following elements:

(1) secure user authentication protocols, as follows:

(A) an authentication protocol that has the following features:

(i) control of user IDs and other identifiers;

(ii) a reasonably secure method of assigning and selecting passwords or use of unique identifier technologies, such as biometrics or token devices;

(iii) control of data security passwords to ensure that such passwords are kept in a location and format that do not compromise the security of the data they protect;

(iv) restricting access to only active users and active user accounts; and

(v) blocking access to user identification after multiple unsuccessful attempts to gain access; or

(B) an authentication protocol that provides a higher level of security than the features specified in subdivision (A) of this subdivision (c)(1).

(2) secure access control measures that:

(A) restrict access to records and files containing personally identifiable information to those who need such information to perform their job duties; and

(B) assign to each person with computer access unique identifications plus passwords, which are not vendor-supplied default passwords, that are reasonably designed to maintain the integrity of the security of the access controls or a protocol that provides a higher degree of security;

(3) encryption of all transmitted records and files containing personally identifiable information that will travel across public networks and encryption of all data containing personally identifiable information to be transmitted wirelessly or a protocol that provides a higher degree of security;

(4) reasonable monitoring of systems for unauthorized use of or access to personally identifiable information;

(5) encryption of all personally identifiable information stored on laptops or other portable devices or a protocol that provides a higher degree of security;

(6) for files containing personally identifiable information on a system that is connected to the Internet, reasonably up-to-date firewall protection and operating system security patches that are reasonably designed to maintain the integrity of the personally identifiable information or a protocol that provides a higher degree of security;

(7) reasonably up-to-date versions of system security agent software that must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions and is set to receive the most current security updates on a regular basis or a protocol that provides a higher degree of security; and

(8) education and training of employees on the proper use of the computer security system and the importance of personally identifiable information security.

(d) Enforcement.

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

(2) The Attorney General has the same authority to adopt rules to implement the provisions of this chapter and to conduct civil investigations, enter into assurances of discontinuance, and bring civil actions as provided under chapter 63, subchapter 1 of this title. (Added 2017, No. 171 (Adj. Sess.), § 2, eff. Jan. 1, 2019.)

Appendix D

9 V.S.A. § 2431:
Acquisition of brokered personal information; prohibitions

The Vermont Statutes Online
Title 9: Commerce And Trade
Chapter 062: Protection Of Personal Information
Subchapter 001: General Provisions

(Cite as: 9 V.S.A. § 2431)

[Section 2431 effective January 1, 2019.]

§ 2431. Acquisition of brokered personal information; prohibitions

(a) Prohibited acquisition and use.

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

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

(A) stalking or harassing another person;

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

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

(b) Enforcement.

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

(2) The Attorney General has the same authority to adopt rules to implement the provisions of this section and to conduct civil investigations, enter into assurances of discontinuance, bring civil actions, and take other enforcement actions as provided under chapter 63, subchapter 1 of this title. (Added 2017, No. 171 (Adj. Sess.), § 2, eff. Jan. 1, 2019.)