DAVIS GILBERT

Happy New Year, Data Brokers! Now, Register with Vermont

The Bottom Line

- Vermont's law governing data brokers takes effect in a few days.
- If you think you are a data broker who falls within the law, now is the time to take all steps necessary to comply.

With only days to go before Vermont's data broker regulation law takes effect, the Vermont Attorney General has finally issued guidance that explains how businesses can comply with the law and the nature of the obligations it imposes on them.

The Vermont Statute

This past May, the Vermont legislature passed the first law in the United States specifically regulating data brokers, effective January 1, 2019. Data brokers must register with the state by January 31, 2019, and annually thereafter, and must provide specified information to the state when they register.

The law also imposes certain minimum data security standards on data brokers, and prohibits data brokers — and everyone else — from acquiring certain personal information of consumers through fraudulent means or with the intent to commit wrongful acts.

What Is a Data Broker?

As we discussed in a previous Alert, the Vermont law defines "data broker" as a business that knowingly collects and sells or licenses to third parties "brokered personal information" of a consumer with whom the business does not have a direct relationship. The new guidance from the Vermont Attorney General amplifies the definition by listing four questions that can determine if a particular business is a data broker for purposes of the law. If a business answers "yes" to these questions, and if its activities do not fall within certain very limited exceptions, the business is a data broker.

The questions are:

1. Does the business handle the data of consumers with whom it does not have a direct relationship?

Data brokers collect and sell or license the data of consumers with whom they do not have a direct relationship. For example, a retailer that sells information about its own customers is not a data broker because it has a relationship with its customers.

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

A business that collects data for its own use or analysis is not a data broker. As an example, an insurance company that buys data about individuals to set rates and develop new products but that does not resell or license the data, is not a data broker.

The guidance makes clear that "collection" is a broad term, and can include the purchase or license of data from someone else, or the collection from original sources such as court records, surveys, or internet search histories.

According to the guidance, 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 does not include a sale or license that is "merely incidental to the business."

3. Is the data about individuals residing in Vermont?

Vermont's data broker regulation does not apply to a company that has no data on Vermont residents or who is not otherwise subject to jurisdiction in Vermont. Importantly, the guidance suggests that a national data broker has a "non-trivial chance" of possessing Vermonters' data. It states that if a data broker does not maintain the state of residence of individuals whose data it collects, it might presume that there may be at least one Vermonter in its data set.

4. Is the data brokered personal information (BPI)?

BPI is defined broadly. It must be computerized as well as categorized or organized for dissemination to third parties. According to the guidance, data is BPI if it contains one or more of a person's name, address, date of birth, place of birth, mother's maiden name, biometric information, name or address of a member of the consumer's immediate family or household, or Social Security number or other government-issued identification number.

The guidance also provides that BPI includes "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."

By contrast, BPI does not include publicly available information 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.

Registration

Data brokers must register with the Vermont Secretary of State by January 31, 2019, and every year thereafter.

As part of the registration process, a data broker must provide information that includes the name of a contact person and its own physical, email, and internet addresses.

In addition, if it permits consumers to opt-out of its collection of BPI, opt-out of its databases, or opt-out of certain sales of data, it must provide the method for requesting an opt-out. If the opt-out applies to only certain activities or sales, it must explain which ones, and it must indicate if it permits consumers to authorize third parties to perform the opt-out on their behalf.

Moreover, a data broker must specify the data collection, databases, or sales activities from which consumers may not opt-out.

It is important to recognize that the data broker regulation does not require data brokers to permit consumers to opt-out of collection, sales, or storage activities, but only requires that data brokers that do permit opt-outs describe how consumers can do so.

As part of the registration process, a data broker also must explain whether it has implemented a purchaser credentialing process. Notably, the regulation does not require that a data broker have a credentialing process, but that it state whether it does.

In addition, the registration process requires that a data broker set forth the number of security breaches involving BPI that it experienced during the prior year and, if known, the total number of consumers affected by the breaches.

Finally, if a data broker has actual knowledge that it possesses BPI of minors, it also must detail the data collection practices, databases, sales activities, and opt-out policies applicable to that information.

A data broker required to register that fails to do so is subject to a penalty of $50 per day, beginning February 1, 2019, up to a maximum of $10,000 per year.

Data Security Standards

The guidance makes clear that data brokers have a duty under the law to protect consumers' personally identifiable information (PII), just as other businesses must do under current Vermont law. In addition to developing, implementing, and maintaining a comprehensive security program that is in writing and taking numerous other steps to protect PII, a data broker, involving the sale or licensing of PII, also must implement the following computer system requirements:

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

Prohibition on Acquisition of Personal Information

The law prohibits any business or individual, not just data brokers, from acquiring personal information through fraudulent means and acquiring BPI for the purpose of stalking, harassing, engaging in unlawful discrimination or committing fraud.

Related People

Gary Kibel
Partner
212 468 4918
gkibel@dglaw.com