

PUBLICATION

New Data Law Comes into Effect on January 1, 2019 – Does Your Business Have to Comply?

Authors: Aldo M. Leiva, Alisa L. Chestler

November 08, 2018

Does your company qualify as a "data broker"? You may be surprised by the answer and as of January 1, 2019 your company may be subject to a new Vermont law governing such entities. Vermont will be the first state in the United States that will directly regulate any "data brokers" that process the personal information of consumers that reside in the State by imposing annual registration and security breach disclosure requirements. Businesses must be aware of the requirements to assess whether it must register as soon as possible.

The statute broadly defines a "data broker" as a business that knowingly collects and sells or licenses the personal information of any Vermont resident. A direct relationship with the individual does not need to exist for the law to apply. Specifically, the business must sell or license brokered personal information as defined by the law. The statute excludes from this definition any businesses that collect information from their own customers, employees, users, or donors.

Any business that meets the definition of "data broker" shall be required to formally register with the Vermont Secretary of State and disclose information regarding use of Vermont consumer data which will require the data broker to identify and document data collection practices. Data brokers will also need to document and annually report details of opt-out procedures identification of specific data collection practices from which the consumer may not opt out, and the number of security breaches experienced during the prior year and the total number of affected consumers, if known.

The law also requires the development and implementation of a comprehensive information security program to protect personal information, and while similar to many state laws with similar requirements, there are specifics that should be understood by all covered by the law.

Failure to comply with the above requirements results in civil liability and exposes businesses to allegations of unfair and deceptive trade practices.

If you have any questions regarding these issues or any other data privacy or security breach related issues, please contact [Alisa Chestler](#), [Al Leiva](#), or any attorney in Baker Donelson's [Data Protection, Privacy and Cybersecurity Group](#).