BRACEWELL

INSIGHTS

Virginia Is For [Data Privacy] Lovers: Introduction to Virginia's New Consumer Protection Law

December 7, 2021

By: ***Lucy Porter*** ***Matthew G. Nielsen***

On January 1, 2023, the ***Virginia Consumer Data Protection Act*** (VCDPA) will go into effect. With passage of the law earlier this year, Virginia joined ***Colorado*** and California as the only states to enact comprehensive privacy legislation. The VCDPA includes components similar to the California Privacy Rights Act (CPRA), including providing certain rights to Virginia residents, creating obligations for companies doing business in Virginia, and giving significant enforcement authority to the Virginia Attorney General. However, like the Colorado Privacy Act (CPA) discussed in a previous client alert, the VCDPA does not include employee personal data. Organizations should kickstart compliance efforts now to avoid regulatory scrutiny.

Covered Businesses and Applicability

Covered Entities. Similar to the CPRA, the VCDPA establishes thresholds to determine applicability. In particular, the VCDPA applies to entities that conduct business in Virginia or produce products or services targeted towards Virginia residents and that control or process personal data of at least:

(1) 100,000 consumers during the calendar year or

(2) 25,000 consumers and derive over 50% gross revenue from the sale of personal data.

Unlike the CPRA, there is no revenue threshold which means that large businesses that don't meet these requirements can avoid obligations under the VCDPA. The VCDPA also provides exemptions for: (1) Virginia State agencies and bodies, (2) financial institutions or data subject to Gramm-Leach-Bliley Act, (3) entities covered under HIPAA and the Health Information Technology for Economic and Clinical Health Act, and (4) institutions of higher education.

Covered Individuals. A "consumer" is a person who is a resident of Virginia "acting only in an individual or household context." The definition goes on to expressly exempt a person acting in a "commercial or employment" context. This is an important distinction not present in the CPRA, which is set to apply to employee data on January 1, 2023.

Personal and Sensitive Data. The VCDPA defines "personal data" broadly as "any information that is linked or reasonably linkable to an identified or identifiable" person. Two exemptions are provided for publicly available information and de-identified data. Similar to the GDPR and the CPRA, the VCDPA also regulates "sensitive data." Sensitive data is defined as a category of personal data that includes: (i) personal data revealing racial or ethnic origin, religious beliefs,

mental or physical health diagnosis, sexual orientation or citizenship or immigration status; (ii) genetic or biometric data for the purpose of uniquely identifying a natural person; (iii) personal data collected from a known child; or (iv) precise geolocation data. The protections for sensitive data are discussed further below.

Controller and Processor Obligations

Similar to the GDPR, the VCDPA differentiates between Controllers (companies that are responsible for determining the purpose and means of processing personal data) and Processors (companies that process personal data on Controllers' behalf). Generally, a Processor is obligated to adhere to the instructions of a Controller and to assist the Controller in meeting the Controller's obligations under the VCDPA. Written contracts between Controllers and Processors are required prior to processing personal data.

A Controller is required to abide by several key obligations, including:

- Providing privacy notices to consumers describing the Controller's data processing practices and consumers' rights;
- Establishing and implementing reasonable data security practices to protect personal data;
- Limiting the collection of personal data to what is reasonably necessary for the purpose for which the data is processed;
- Obtaining consumer consent before processing any sensitive data;
- Responding to consumer rights requests; and
- Conducting Data Protection Assessments in certain circumstance, including the sale of personal data, the processing of personal data for purposes of targeted advertising or profiling, the processing of sensitive data and any processing activities involving personal data that present a heightened risk of harm to consumers.

Consumer Rights

The VCDPA provides consumers with rights of access, correction, deletion, and portability, as well as the right to opt out of certain data processing. Entities are required to respond to requests within 45 days of receipt of the request. The VCDPA also provides consumers a right to opt out of the processing of personal data for purposes of targeted advertising, the sale of their personal data to third parties, and profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer. In contrast to the CPRA, Virginia consumers may only opt-out of the sale of personal data if the data is exchanged for monetary consideration. However, both the VCDPA and CPRA provide consumers an explicit opt-out right for certain forms of targeted advertising and profiling.

Enforcement of the VCDPA

The Virginia Attorney General will retain exclusive authority to enforce the VCDPA. This includes authority to initiate investigations into Controllers and Processors. Unlike the CPRA, however, no private right of action is provided in the VCDPA, and the text expressly precludes interpretation to support an implied right of action. Violations of the VCDPA can result in civil

penalties of up to $7,500 for each violation as well as any reasonable expenses incurred by the government in investigating and preparing the case. This includes attorney fees.

Key Takeaways

State-level momentum for comprehensive privacy legislation is at an all-time high. And responsibilities of organizations will continue to expand as long as consumer data rights are increasing. Although the VCDPA does not go into effect until January 2023, organizations should begin preparations now as non-compliance can be costly. Preparatory steps include:

- Determine whether the VCDPA will apply to your business;
- Understand the consumer data your business processes; and
- Consult with experienced professionals.

Bracewell lawyers are prepared to assist and provide the guidance your organization needs to avoid potential fines or other privacy-related hiccups.

This alert is the third in a series reviewing the ***2021 data privacy legislation landscape***. Stay tuned for our next piece breaking down the California Privacy Rights Act.