BROOKS PIERCE

Virginia Becomes the Second State—and the First on the Eastern Seaboard—to Adopt a Comprehensive Data Protection Law

03.31.2021

In March of 2021, Virginia became the second state to adopt a comprehensive data protection law. The Virginia Consumer Data Protection Act (VCDPA), which goes into effect on Jan. 1, 2023, borrows many concepts from the California Consumer Privacy Act (CCPA), which went into effect in 2020, but has enough subtle difference that companies doing business in both California and Virginia will need to evaluate whether they have different or unique compliance obligations under each state's law.

For many East Coast businesses who did not have to focus on California law, the VCDPA is likely to bring new and daunting privacy compliance concepts that will take substantial effort to meet over the next two years. This alert highlights some of the key aspects of the VCDPA that any company doing business in Virginia should be aware of moving forward.

Who has to comply with the VCDPA?

The VCDPA applies to any company that does business in Virginia or that "produce[s] products or services that are targeted to" Virginia residents where that company, either:

1. controls or processes "personal data" of at least 100,000 Virginia residents; or
2. controls or processes "personal data" of at least 25,000 Virginia residents and derives more than 50% of its gross revenue from the sale of personal data.

While these are similar concepts to the CCPA, the VCDPA does not have a standalone revenue threshold that would subject companies with large amounts of revenue and only a handful of Virginia customers to its requirements.

In similar fashion to the CCPA, the VCDPA exempts certain types of entities from needing to comply, as follows: (i) Virginia state government entities; (ii) financial institutions with data subject to the Gramm-Leach-Bliley Act (GLBA); (iii) covered entities or business associates subject to the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act; (iv) non-profits; and (v) institutions of higher education.

What is "Personal Data" under the VCDPA?

The definition of "personal data" is broad and includes any information that is "linked or reasonably linkable to an identified or identifiable natural person."

There are, however, a number of important exemptions from the definition. The first includes certain types of data that are otherwise addressed by federal or other Virginia state laws. Examples include data subject to GLBA, HIPAA, and other similar industry focused data protection laws.

A second, and very significant exemption for many business, is employment data, which includes application data, information necessary to administer benefits programs, and emergency contact information kept by business entities. Employment data is not currently excluded under the CCPA, which has been a point of consternation for many businesses.

A third exemption exists for de-identified or pseudonymous data.

Finally, publicly available information is not "personal data" under VCDPA.

How does the VCDPA protect consumer personal data?

One of the main goals behind the VCDPA, like the CCPA, was to provide a set of previously unobserved privacy rights, including the right to access, correct and delete personal data, to Virginia residents. Consumers also have a right to request their data from a business in a format that can be transferred to another business of the consumer's choosing—often known as the right to data portability.

When it comes to how a business uses a consumer's data, the VCDPA provides users the right to opt out of data processing for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling to make decisions that would produce legal or similarly significant effects to a consumer.

In another departure from the CCPA, the VCDPA defines "sale" to specifically reference an exchange of personal data "for monetary consideration." This is much clearer than the broad CCPA definition that could potentially include any transfer of personal data where the transferor receives value. The definition of a sale also explicitly excludes a transfer to affiliates of the controlling business.

The right to opt out of profiling is a new concept in American privacy law that borrows heavily from concepts expressed in Europe's General Data Protection Regulation (GDPR). The VCDPA defines "profiling" as "any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements." Businesses using predictive screening processes, and similar automated processes, will have to consider how they will provide this right to consumers.

The VCDPA provides special rights and protections to "sensitive" personal data, which is defined to include (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 processed for the purpose of uniquely identifying a natural person; (iii) the personal data collected from a known child; and (iv) precise geolocation data. Most significantly, businesses must obtain affirmative consent before processing a consumer's sensitive personal data.

What must businesses do to comply with the VCDPA?

In short, quite a lot, if the law applies and the business has not already made changes to comply with the CCPA or GDPR. As a start, businesses must ensure their privacy notices (or policies) include statements addressing, at a minimum:

- the purpose(s) for which the business processes personal data;
- how a consumers may exercise the individual rights provided by the VCDPA, including how a consumer may appeal a business' decision with regard to the consumer's request;
- the categories of personal data that the business shares with third parties, if any;
- the categories of third parties, if any, with whom the business shares personal data;
- a clear disclosure and information on how to opt out if the business sells personal data to third parties or processes personal data for targeted advertising

From an operational standpoint, businesses must limit their data collection to what is practical and reasonable under the circumstances and "establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data" that is collected.

Businesses that process any form of sensitive personal data or that engage in data processing for certain purposes, such as targeted advertising, the sale of personal data, or profiling, must conduct a "data protection assessment" to evaluate the risks associated with their processing activities. These assessments must weigh the overall benefits of the processing activity against the potential

risks to the rights of the consumer, as mitigated by applicable safeguards.

Finally, businesses that engage third parties to process data must ensure that their data processing agreements meet minimum adequacy requirements. For example, these agreements must include confidentiality and retention clauses, among others, and must "clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties."

How is the VCDPA going to be enforced?

The Virginia Attorney General has exclusive authority to enforce the VCDPA, though violators must be given notice and a chance to cure any alleged violations within 30-days before the attorney general may seek injunctive relief or monetary damages. Violations carry statutory damages up to $7,500 for each violation, as well as "reasonable expenses incurred in investigating and preparing the case, including attorney fees."

Notably, there is no private right of action under the VCDPA.

What should businesses do to comply?

While the effective date of Jan. 1, 2023 may seem far off, businesses that foresee a need to comply with the law—either now, or because of projected growth over the next few years—should seriously consider budgeting and planning to comply now. Compliance with privacy regimes almost always tends to be more time and resource intensive than C-suite executives imagine. Bringing information technology and security personnel into the discussion early will help to minimize the squeeze that many businesses felt in trying to comply with the CCPA at the last minute.

Additionally, while the CCPA and VCDPA hold unique positions now as the first and second comprehensive data protection laws in the United States, no privacy professional thinks that is likely to be the state of affairs for long. Several other states are currently considering their own versions of comprehensive privacy laws—any one of which could require compliance by an earlier date.

Reach out to the privacy and data security team at Brooks Pierce to determine if the VCDPA applies to your business and to get assistance with an early start on the compliance process.

PEOPLE

Will Quick

SERVICES

Privacy