NOW + NEXT

PRIVACY ALERT | NIXON PEABODY LLP

MARCH 5, 2021

The Virginia Consumer Data Protection Act—What businesses need to know

By Eliza Davis and Anders van Marter

On March 2, 2021, Virginia became the second state to enact comprehensive privacy regulation. California passed the California Consumer Privacy Act (CCPA) in 2018 and recently extended privacy protections in the California Privacy Rights Act (CPRA). The Virginia Consumer Data Protection Act (VCDPA) is another example of the expansion of data privacy in the U.S. There is considerable overlap between the VCDPA and the CPRA, as well as similarities between the VCDPA and the European General Data Protection Regulation (GDPR). There are also some differences between the VCDPA and the other privacy laws, which companies need to make sure to consider to ensure compliance.

What does this mean for businesses? Here are a few key points.

A compliance runway

The VCDPA goes into effect on January 1, 2023, so businesses have time to prepare and update their compliance programs.

Whom does it apply to?

The VCDPA applies to organizations that conduct business in Virginia or produce products or services that target Virginia residents and that:

- Control or process personal data of at least 100,000 consumers in a calendar year; or
- Control and process personal data of at least 25,000 consumers and derive over 50% of gross revenue from the sale of personal data.

Compared to the CCPA, the VCDPA doubles the amount of consumer data that must be collected or processed for a business to fall within its scope.

Scope

The VCDPA, like the CPRA and GDPR, includes a broad definition of personal data: "any information that is linked or reasonably linkable to an identified or identifiable natural person." Notably, the VCDPA's definition does not include de-identified data or publicly available information. The VCDPA defines "public information" to include information that is "lawfully made available through federal, state, or local government records" and "information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media . . . unless the consumer has restricted the information to a specific audience."

Notable exemptions

The VCDPA includes many exemptions, including:

- Governmental entities;
- Nonprofits;
- Employee data;
- Information that is governed by federal regulations, such as the Family Educational Privacy Protection Act, Fair Credit Reporting Act, and Children's Online Privacy Protection Act;
- Financial institutions and data subject to the Gramm-Leach-Biley Act;
- Covered entities and data governed by the Health Insurance Portability and Accountability Act; and
- Higher education institutions.

Consumer rights

Borrowing from both the CPRA and the GDPR, the VCDPA provides consumers with several rights, including the right to:

- Opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or profiling;
- Amend inaccuracies;
- Data deletion; and
- Data portability.

Data controller obligations

Similar to the GDPR, Virginia's law establishes "controller" and "processor" roles, which differentiate how entities handle personal data. Controllers are those who determine the purposes and means of processing personal data, while processors are entities that process personal data on behalf of a controller and at the controller's direction. The law assigns different obligations based on an entity's status as a controller or processor. The VCDPA imposes several obligations on controllers, including:

- Establishing, implementing, and maintaining reasonable administrative, technical, and physical data security practices to protect confidentiality, integrity, and accessibility of personal data;
- Providing consumers with privacy notices;
- Contractual requirements in engaging data processors; and

- Conducting data protection assessments.

Sensitive data

Another concept borrowed from the GDPR is the requirement that controllers obtain consumers' informed consent before processing "sensitive data." Sensitive data include:

- Personal data revealing racial or ethnic origin; religious beliefs; mental or physical health; sexual orientation; or immigration status
- Genetic or biometric data
- Data collected from a child (a person younger than 13); and
- Geolocation data

Importantly, the CPRA includes a sensitive data category, but requires businesses to provide consumer with the ability to *opt out* of the processing of sensitive data. The VCDPA, on the other hand, requires consumers to *opt in*.

Enforcement

The VCDPA does not provide for a private right of action; enforcement is solely through the attorney general. If the attorney general decides to take action, the office must notify the controller, which then has 30 days to cure the violation and provide the attorney general with an "express written statement that the alleged violations have been cured and that no further violations shall occur." If a controller fails to cure a violation, it could face up to $7,500 per violation.

Looking ahead

In preparing to comply with both the CPRA and VCDPA, companies will have to navigate the convergence and diversion between the two laws, which could be difficult. Fortunately, both the CPRA and VCDPA provide a two-year ramp-up period, giving businesses time to understand their compliance obligations. As other states, such as Washington, consider privacy regulations, companies will have to continue to be diligent to understand the nuances to ensure compliance. Nixon Peabody will continue to monitor and report on developments as the privacy landscape continues to shift.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

- Eliza Davis, 312-977-4150, etdavis@nixonpeabody.com
- Anders van Marter, Senior eDiscovery Specialist, 312-977-9215, avanmarter@nixonpeabody.com
- Jason Gonzalez, 213-629-6019, jgonzalez@nixonpeabody.com
- Jeffrey Costellia, 202-585-8207, jcostellia@nixonpeabody.com
- Sarah Swank, 202-585-8500, sswank@nixonpeabody.com
- Alycia Ziarno, 202-585-8265, aziarno@nixonpeabody.com