Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What A New Virginia Privacy Law Could Mean For Businesses


Greg Parks


Kristin Hadgis


Drew Jordan


Taylor Day

By **Greg Parks, Kristin Hadgis, Drew Jordan and Taylor Day**
(February 23, 2021, 4:42 PM EST)

Virginia is on track to become the second state in the U.S. to pass a comprehensive data privacy law after the Virginia Consumer Data Protection Act, or VCDPA, quickly passed both houses of Virginia's Legislature earlier this month with overwhelming bipartisan support.

The Virginia House of Delegates adopted the VCDPA, H.B. 2307, on Jan. 29, and the Virginia Senate approved an identical companion bill, S.B. 1392, on Feb. 5.

The VCDPA has a number of key similarities to the California Consumer Privacy Act, or CCPA; the California Privacy Rights Act, or CPRA, which comes into effect in 2023; and the European Union's General Data Protection Regulation, or GDPR, and it follows a similar framework to proposed data privacy bills pending in other statehouses.

After reconciliation of the two bills — likely a formality given that each bill is identical — it will be sent to Virginia Gov. Ralph Northam's desk to be signed into law. If passed, the legislation will take effect on Jan. 1, 2023, and will require companies doing business in Virginia to reassess their collection and use of consumer personal information and modify their business practices to account for Virginia's new requirements.

The Virginia CDPA, if signed into law, would make Virginia the second state in the U.S. with a comprehensive privacy law after California. This article details a few noteworthy features of the VCDPA and highlights steps that businesses should take to ensure compliance if the bill becomes the law.

Covered Businesses and Applicability

In its current form, the VCDPA would apply to all persons who conduct business in the commonwealth of Virginia or "produce products or services that are targeted to residents of the Commonwealth" and, during a calendar year, either (1) control or process personal data of at least 100,000 consumers, or (2) derive over 50% of gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers.

The bill defines "personal data" as "any information that is linked or reasonably linkable to an identified or identifiable natural person." Personal data does not include publicly available information or de-identified data.

Notably, the term "consumer" means a natural person who resides in Virginia and does not include any person acting in a commercial or employment context. This is a departure from the CCPA and GDPR, which do have at least some provisions that apply to a natural person acting in a commercial or employment context.

This means that for purposes of the Virginia CDPA, controlling or processing personal data in the business-to-business or employment context falls outside the scope of the current version of the VCDPA.

It also is notable that "publicly available information" is defined much more broadly than under the CCPA, such that "personal data" that is protected is narrower under the proposed Virginia law than under California's law.

The proposed bill contains a number of notable carveouts similar to, but broader than, those in the CCPA, with both entity and data-specific exemptions.

If signed into law, financial institutions subject to the Gramm-Leach-Bliley Act, covered entities or business associates subject to the Health Insurance Portability and Accountability Act, higher education institutions, nonprofit organizations and commonwealth agencies would all be exempt from the VCDPA.

The proposed legislation would also exempt particular categories of data, including any data already regulated by certain federal laws such as HIPAA, Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Family Educational Rights and Privacy Act, and the Children's Online Privacy Protection Act.

While the VCDPA borrows from the CCPA in terms of using threshold requirements to determine which businesses must comply with the act, the absence of a standalone revenue threshold, such as the $25 million annual gross revenue threshold present in the CCPA, most likely means that Virginia's bill will apply to far fewer businesses than are presently subject to the CCPA.

The VCDPA also defines a "consumer" more narrowly than the CCPA or CPRA by permanently excluding any persons acting in a commercial or employment context.

Taken together, the absence of any independent revenue threshold and a narrow definition of consumer generally means that fewer businesses will be subject to the VCDPA than California's privacy regime.

Consumer Rights

The VCDPA would grant Virginia consumers certain rights relating to their personal data controlled or processed by covered entities. Specifically, consumers would be afforded the rights of access, correction, deletion and portability of their personal data.

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.

These rights will be similar to those afforded by the CCPA once the CPRA becomes effective in 2023. With respect to the sale of personal data, the VCDPA's opt-out requirements only apply if the data is exchanged by a controller to a third party for monetary consideration.

In situations where personal data is shared and no money is exchanged between the business and the third party, a consumer cannot opt out of the sharing of their personal data. In contrast, under the CCPA and CPRA, a consumer may opt out of a business's sharing of personal information for certain purposes even where no money is exchanged.

However, both Virginia's CDPA and the CPRA provide consumers with an explicit opt-out right extended to certain forms of targeted advertising and profiling.

Under the proposed bill, data controllers are required to respond to a consumer's request to exercise their consumer rights within 45 days of receipt of the request, with one 45-day extension period permitted when "reasonably necessary."

Limited exceptions exist under the current VCDPA for when controllers must comply with consumer right requests, including instances when complying with the request would both be unreasonably burdensome and the controller does not sell personal data or voluntarily disclose it to any third party other than a processor.

Data Controller Responsibilities

The current version of Virginia's CDPA mandates that data controllers limit the collection of personal data to what is adequate, relevant, and reasonably necessary for the purposes for which the data is processed. To safeguard that information, data controllers must establish, implement and maintain reasonable administrative, technical and physical data security practices that are appropriate to the volume and nature of the personal data at issue.

Like the CPRA, additional responsibilities are imposed on data controllers with respect to sensitive data, which is defined as (1) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status, (2) personal data collected from a child, (3) genetic or biometric data or (4) precise geolocation data.

When processing sensitive data, the bill would require controllers to seek consent from consumers. Under the VCDPA, consent is defined as a "clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement" to process their personal data.

This establishes a higher standard than that required under the CPRA and shares more in common with the consent standard established by the GDPR.

Some consumer privacy advocacy groups have favored this sort of opt-in approach to consent, in contrast to the opt-out approach reflected in the CCPA and CPRA.

In the case of children's data, the bill allows data controllers to obtain parental consent in accordance with the Children's Online Privacy Protection Act.

Data controls would also be required under the VCDPA to provide consumers with reasonably accessible privacy notices that clearly disclose the categories of personal data collected; the purpose for the

collection; the categories of personal data the controller shares with third parties, if any; and how consumers can exercise their rights.

To exercise those consumer rights afforded under the VCDPA, consumers must be allowed to submit requests to data controllers without needing to create an account with the data controller.

Data Protection Assessments

Like the CPRA, Virginia's proposed CDPA requires businesses to conduct data protection assessments of any processing activities that involve personal data in the context of the processing of sensitive data; targeted advertising; sale of personal data; profiling, in certain instances; and any other processing activities involving personal data that "present a heightened risk of harm to consumers."

Such assessments are required to weigh the benefits that may flow, directly and indirectly, from the processing to the controller, consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by applicable safeguards.

The attorney general of Virginia has the power to request the disclosure of such data protection assessments without court order. If compelled and produced to the attorney general for evaluation, the assessments are to remain confidential and the VCDPA provides specific provisions that prevent the waiver of attorney-client privilege and work product protection.

Enforcement and Lack of a Private Right of Action

Significantly, the VCDPA does not provide for any private right of action. In fact, private rights of action are expressly barred in the bill.

Instead, under the VCDPA, the attorney general is granted the exclusive right to enforce the law, subject to a 30-day cure period. The attorney general may seek up to $7,500 per violation, injunctive relief and recovery of reasonable expenses incurred in investigating and preparing the case, including attorney fees.

Key Takeaways for Business and Looking Ahead

The current version of the VCDPA reflects principles from the CCPA, the CPRA and the GDPR, and borrows many defined terms from these laws.

Like these other statutes and regulations, the VCDPA broadly defines "personal data," mandates that a business's collection of personal data be relevant and limited only to what is necessary for the business and provides Virginia consumers with a bundle of new rights with respect to their personal data. However, businesses should bear in mind that the VCDPA differs in some significant aspects.

First, unlike the CCPA's limited private right of action for security breaches, Virginia's legislation does not provide for a private right of action. Instead, the attorney general will have the exclusive right to enforce the law.

Practically speaking, this means that Virginia residents will be limited in their ability to sue businesses for alleged violations either in the individual or class action context, leaving enforcement entirely up to the attorney general. It remains to be seen how much of the attorney general's budget will be allocated to

enforcing the VCDPA against businesses.

Second, the VCDPA would impose stricter requirements than the CPRA as to how businesses obtain consent from consumers before processing sensitive data.

While the CPRA accounts for sensitive personal information and permits consumers to submit opt-out requests specific to this sensitive personal information, the Virginia Legislature borrowed the stricter standard from the GDPR and requires a business to obtain affirmative consent before any sensitive data may be collected and processed.

Depending on how the attorney general decides to enforce this standard, businesses should be prepared to build compliance programs that account for Virginia's affirmative consent requirement.

Third, covered businesses that only process consumer requests to opt out of the sale of personal data will need to expand their opt-out compliance programs. If passed, the VCDPA goes further than just granting Virginians the right to opt out of the sale of their personal data and broadens that opt-out right to the use of personal data for targeted advertising and profiling purposes.

The CPRA, which goes into effect on Jan. 1, 2023, similarly endows consumers with a new right to opt out of their personal data being used for cross-context behavioral advertising.

Ultimately, those businesses that have been building compliance programs for the CCPA and CPRA will be well positioned to comply with the Virginia CDPA, should it be signed into law. Some key differences in the VCDPA, however, will require businesses to review their compliance programs to ensure compliance with the nation's second comprehensive privacy state law.

Greg Parks and Kristin Hadgis are partners, and Drew Cleary Jordan and Taylor Day are associates, at Morgan Lewis & Bockius LLP.