WILLCOX SAVAGE

VIRGINIA ENACTS COMPREHENSIVE PRIVACY LAW

CORINA V. SAN-MARINA, CIPP/US
Willcox Savage

On March 2, 2021, Governor Ralph Northam signed the Virginia Consumer Data Protection Act (VCDPA) into law. Virginia is now the second state to enact comprehensive privacy legislation, the first being California with its California Consumer Privacy Act (CCPA) and the California Privacy Rights and Enforcement Act (CPRA). The VCDPA, which will go into effect on January 1, 2023, draws concepts from the CCPA, the CPRA and the European Union's General Data Protection Regulation (GDPR).

Entities and Data Subject to the VCDPA

The VCDPA applies to all entities that "conduct business in the Commonwealth of Virginia or produce products or services that are targeted to residents of the Commonwealth" and that (1) during a calendar year control or process personal data of at least 100,000 Virginia residents or (2) control or process the personal data of at least 25,000 consumers and derive at least 50 percent of its gross revenue from the sale of personal data. (The law does not make clear whether the revenue threshold applies to Virginia residents only.)

Businesses can assume that economic activity that triggers tax liability or personal jurisdiction in Virginia will also trigger VCDPA applicability. Unlike the CCPA, the VCDPA does not include a standalone revenue threshold that imposes obligations, meaning that even large businesses will not be subject to the VCDPA so long as they do not meet one of the other two thresholds.

To determine whether VCDPA is applicable, a business will need to know the type of personal data it controls or processes and whether it engages in the sale of personal data. "Personal data," a GDPR term, is defined to include "any information that is linked or reasonably linkable to an identified or identifiable natural person" but excludes "de-identified" data, publicly available information, pseudonymous data, and employment-related information.

The statute defines "sale of personal data" as "the exchange of personal data for monetary consideration by the controller to a third party," a narrower definition than that in the CCPA, under which a sale occurs where the exchange is also for "other valuable consideration." Excluded from the definition of sale are disclosures made in the ordinary course of business such as disclosures to affiliates, to third parties if requested by consumers, to processors (a GDPR term and equivalent of "service providers" under the CCPA), and disclosures of certain information made public by a consumer.

Exemptions from the VCDPA

The VCDPA provides two types of exemptions, significantly broader than the CCPA's exemptions. Entity-level exemptions covers agencies or political subdivisions, financial institutions subject to the Gramm-Leach-Bliley Act (GLBA), entities subject to the Health Insurance Portability and Accountability Act ("HIPAA"), nonprofit organizations, and institutions of higher education. In addition, there are 14 categories regarding exempted datasets, including specific information regulated by the GLBA, the Fair Credit Reporting Act, the Drivers Privacy Protection Act, the Farm Credit Act, the Family Educational Rights and Privacy Act, and specific employee and job applicant data.

Consumer Rights under the VCDPA

The VCDPA provides consumers with CCPA/GDPR-type rights including (1) the right to access, correct, and delete their personal data, (2) the right to data portability, (3) the right to opt out of processing for purposes of targeted advertising, the sale of personal data, or profiling that results in decisions with legal effects, and (4) the right to appeal a business's denial to act within a reasonable time.

A business that acts as a controller (a GDPR term) must respond to a consumer request within 45 days after receipt, with the option to extend the deadline by an additional 45 days so long as it provides notice and the reason for the extension. If a controller fails to respond to a consumer's request, it must provide a justification for declining to respond and instructions on how to appeal the decision. If the appeal is denied, the controller needs to inform the consumers how they can submit a complaint to Virginia's attorney general.

Controller Responsibilities under the VCDPA

The VCDPA limits a controller's collection and use of personal data and requires the implementation of reasonable technical and organizational safeguards. Controllers can collect and process only personal data that is reasonably necessary and compatible with the purposes previously disclosed to consumers and obtain consent before processing personal data collected for a different purpose.

Departing from the CCPA, the VCDPA gives consumers the right to opt in to the processing of their sensitive data, which is defined as: "personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; genetic or biometric data processed for the purpose of uniquely identifying a natural person; the personal data collected from a known child; and precise geolocation data."

Controllers are required to provide a privacy notice that explains how consumers can exercise their rights, how they can opt out of the sale or processing of their personal data for targeted advertising, the categories of personal data processed, the purpose for processing personal data, the categories of personal data shared with third parties, and the categories of third parties with whom controller shares personal data.

Additional GDPR-Type Obligations for Controllers and Processors

The VCDPA requires controllers to conduct "data protection assessments" to evaluate the risks associated with processing personal data for purposes of targeted advertising, the sale of personal data, the processing of sensitive data, the processing of personal data for purposes of certain profiling activities, and any processing activities that pose a heightened risk of harm to consumers.

In addition, controllers must enter into data-processing agreements with their processors setting 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. The agreement should also include certain confidentiality and retention provisions and obligations on processors to cooperate with controllers and demonstrate that they have policies and technical and organizational measures to meet their own obligations.

Enforcement—No Private Right of Action

Only the Virginia attorney general is authorized to enforce the VCDPA, subject to a 30-day cure period. The attorney general may seek injunctive relief, damages of up to $7,500 for each violation, and attorneys' fees. Unlike the CCPA, however, the VCDPA does not provide for a private right of action for cybersecurity failures.

Responding to the VCDPA

Even for businesses that have already implemented privacy programs to comply with the GDPR and/or the CCPA, the VCDPA presents new challenges. Such businesses will need to implement: (1) broader affirmative consent or opt-in requirement to process sensitive personal data; (2) broader opt-out rights for processing that covers not only sales of personal data but also targeted advertising and profiling decisions that produce legal or similarly significant effects; (3) mandatory data-protection assessments for sales of personal data; (4) targeted advertising and profiling, processes to comply with the obligation to delete personal data collected about a consumer; and (5) changes to the automated processes already implemented related to consumer requests regarding the mandatory right to an appeal process. In taking those steps, businesses will also need to consult experienced and well-qualified privacy counsel to ensure that they are meeting all of the relevant requirements of this new Virginia law.