TRAUB LIEBERMAN

CYBER LAW BLOG

March 22, 2021

A Summary of Virginia's Recently Enacted Comprehensive Consumer Data Privacy Act (VCDPA)

BY: Jason Taylor

On March 2, 2021, Virginia became the second state to enact a comprehensive data privacy law, following only California and the California Consumer Privacy Act ("CCPA"). While the Virginia Consumer Data Privacy Act ("VCDPA") is similar in many respects to the CCPA, there are some differences. The act also borrows from the newly enacted California Privacy Rights and Enforcement Act as well as elements of the European Union's General Data Protection Regulation ("GDPR"). While the VCDPA does not take effect until January 1, 2023, we take a look at some of the key provisions, and comparisons with other data protection laws below.

Scope of the VCDPA and Exemptions

Generally, the VCDPA applies to "persons" that conduct business in Virginia or produce products or services that are targeted to residents of the Commonwealth, that either (a) control or process personal data of greater than 100,000 residents; or (b) control or process personal data of greater than 25,000 residents *and* derive over 50% of gross revenue from the sale of personal data. Thus, unlike the CCPA, the Virginia law does not set a revenue threshold to determine applicability for companies that store consumer data. Instead, if an entity falls into either of the two categories above, the VCDPA will apply.

The VCDPA does exempt several entities, including Virginia public entities, entities covered by the Gramm-Leach-Bliley Act, HIPAA-covered entities, nonprofit organizations and higher education institutions.

The VCDA also exempts certain information and data including:

- Protected health information under HIPPA;
- Personal data regulated by the federal Family Education Rights and Privacy Act;
- Certain employer data including data maintained in the course of an individual being employed by a business, as emergency contact information, or necessary to administer benefits; and
- Other health-related data under various regulatory provisions.

Personal Data Rights of Consumers

The VCDPA provides consumers the right to access, delete, correct inaccuracies, and obtain a copy of personal data from controllers of their data. The Act does not provide any express exceptions to these rights. Thus, where a business receives a valid request, the VCDPA mandates that the business comply, regardless of the hardships or impracticable nature of the request.

"Personal data" is defined as any information that is linked or reasonably associated to an identified or identifiable natural person, but excludes de-identified data or publicly available information. This exclusion is significant given the VCDPA's definition of "publicly available information," which includes information that is lawfully made available through federal, state, or local government records, or information that a business has a *reasonable basis* to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information (unless the consumer has restricted the information to a specific audience). This definition introduces a subjective element into a business's reasonable belief such information was lawfully made available to the public.

The VCDPA also provides a right to opt out of the processing of personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

The Act also requires that controllers respond to consumer requests within 45 days of receipt, and if the controller declines to take action regarding the consumer request, it must inform the consumer of the justification for declining to take action and instructions for how to appeal the decision. Moreover, information provided in response to a consumer request must be provided free of charge, up to twice annually per consumer. Controllers may not discriminate against consumers for exercising any of these rights.

Controllers and Processors

Like the GDPR, the VCDPA defines "controllers" and "processors" of consumer data. A "controller" is defined as the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data.

Controllers must limit the collection of personal data to what is "adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed." The VCDPA requires that controllers establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices must be appropriate to the volume and nature of the personal data at issue.

Controllers must also provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

- The categories of personal data processed by the controller;
- The purpose for processing personal data;
- How consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request;
- The categories of personal data that the controller shares with third parties, if any; and
- The categories of third parties, if any, with whom the controller shares personal data.

If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing. The VCDPA also requires a controller to establish, and describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights under the Act.

The VCDPA also applies to "processors" of consumer data, which are defined as a natural or legal entity that processes personal data on behalf of a controller. Processors must ensure that each person processing personal data is subject to a duty of confidentiality, and at the termination of services delete or return all personal data to the controller, among other obligations.

Sale of Personal Data

The act defines the sale of personal data as the "exchange of personal data for monetary consideration by the controller to a third party." This is notable in that it differs from the CCPA, which expands the scope of "sale" to include exchanges for monetary consideration or "other valuable consideration." The VCDPA's definition also only includes the word "sale" – not rent, release, disclose, disseminate, transferring, or otherwise communicating – like the CCPA.

The "sale of personal data" excludes certain exchanges of personal data from a sale, such as:

- Disclosures to processors;
- Disclosures to a third party for purposes of providing a product or service requested by the consumer;
- Disclosures or transfers of personal data to an affiliate of the controller;
- Disclosures of information that the consumer intentionally made available to the general public via mass media channel and did not restrict to a specific audience; and
- Disclosures or transfers to a third party as an asset as part of a merger, acquisition, or bankruptcy.

Sensitive Personal Data

The VCDPA creates a heightened class of personal data called "sensitive data" that includes personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship, or immigration status; the processing of genetic or biometric data for the purpose of uniquely identifying a natural person; personal data collected from a known child; or precise geolocation data.

Controllers must obtain a consumer's affirmative consent before processing sensitive data.

Data Protection Assessments

The VCPDA requires controllers to conduct data protection assessments to identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing. The processing activities involved in such assessments include processing of personal data for purposes of targeted advertising; sale of personal data; processing of personal data for certain types of profiling; processing of sensitive data; and any processing activities involving personal data that present a heightened risk of harm to consumers.

Data protection assessments conducted for the purpose of compliance with other laws or regulations may comply with this requirement if they are reasonably comparable in scope and effect.

The Attorney General may request that a controller disclose any data protection assessment that is relevant to an investigation/investigative civil demand, which the controller is obligated to disclose, and may evaluate the data protection assessment for compliance with the responsibilities set forth in the act.

Notably, these requirements do not apply retroactively, but only to processing activities created or generated after January 1, 2023.

Enforcement & Penalties

Unlike the CCPA, the VCDPA does not include a private right of action for consumers. The Attorney General retains exclusive authority to enforce the VCDPA by bringing an action in the name of the Commonwealth, or on behalf of persons residing in the Commonwealth. The Attorney General also has the power to issue a civil investigative demand to any controller or processor believed to be engaged in, or about to engage in, any violation of the statute.

Any controller or processor that violates the VCDPA is subject to an injunction and liable for a civil penalty of not more than $7,500 for each violation.

The Attorney General may also recover reasonable expenses incurred in investigating and preparing the case, including attorney fees, of any action initiated under the VCDPA.

Consumer Privacy Fund

The VCDPA also creates in the state treasury a special non-reverting fund known as the Consumer Privacy Fund. All civil penalties collected under the Act are paid into the state treasury and credited to the Fund. Money in the Fund must be used to support the work of the Office of the Attorney General to enforce the provisions of the VCDPA, subject to appropriation. Any money remaining in the Fund, including interest thereon, at the end of each fiscal year does not revert to the State's general fund but must remain in the Fund.

Limitations

The VCDPA does include several limitations that allow controllers and processors to take certain actions that comply with federal, state, or local laws, rules, or regulations, or to comply with a civil, criminal, or regulatory investigation or legal proceedings. The VCDPA also permits cooperation with law-enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations; and to investigate, establish, exercise, prepare for, or defend legal claims. Similarly, the obligations imposed on controllers or processors under the statute do not apply where compliance by the controller or processor would violate an evidentiary privilege under the laws of the Commonwealth.

The VCDPA also does not restrict the ability to provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, or take steps at the request of the consumer prior to entering into a contract.

Controllers and processors are also allowed to collect certain data to conduct internal research to develop, improve, or repair products, services, or technology; effectuate a product recall; or identify and repair technical errors that impair existing or intended functionality.

A controller or processor that discloses personal data to a third-party controller or processor, in compliance with the requirements of the VCDPA, is not in violation of the statute if the third-party controller or processor that receives and processes such personal data is in violation of the act, provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation.

While this summary is not intended as a comprehensive review of the new law, or advice as to how the VCDPA (or any other statute) will affect a specific business, hopefully this summary is helpful in identifying the key provisions of the new act, and how it tracks, or diverges, from the CCPA and GDPR. If you would like additional information regarding these issues, please do not hesitate to contact me or any of our other attorneys at any time.