

The Impact of the Virginia Consumer Data Protection Act

April 07, 2021

On March 2, 2021, the Commonwealth of Virginia enacted the [Virginia Consumer Data Protection Act \(VCDPA\)](#). The new law makes Virginia the second state in the United States to enact a comprehensive data privacy regime, following in the footsteps of the [California Consumer Privacy Act \(CCPA\)](#) of 2018.

Enacted in the spirit of enhanced consumer protection, the VCDPA grants consumers several rights, as well as administrative recourse, regarding how businesses use their personal information. The law places far-reaching responsibilities on how companies access, use, store, share, disclose, or otherwise control or process their clients' personal information. Further, the law establishes new requirements for how companies communicate with, and respond to, their clients, as well as how they conduct business with third-party vendors involving client data.

Although the VCDPA does not take effect until January 1, 2023, companies should spend time reviewing and understanding the ins-and-outs of the new law and its applicability to their business. Companies subject to the VCDPA will have to develop and implement new policies and procedures, make changes to their testing, monitoring, and audit programs, and train their front-line employees. If companies fail to abide by the new law's requirements, the penalties can be costly.

Who does the VCDPA protect and who must comply with its requirements?

The scope of the law can be thought of in two ways. First, in terms of who the law protects: Virginia consumers and their personal data. Second, in the requirements placed on businesses tasked with the responsibility of implementing the new consumer protections under the VCDPA.

1. **Consumers:** A "consumer" protected under the law is defined as "a natural person, who is a resident of Virginia, acting only in an individual or household context." Additionally, a consumer's "personal data" means "any information that is linked or reasonably linkable to an identified or identifiable natural person [and] does not include de-identified data or publicly available information."
2. **Businesses Subject to the VCDPA:** The VCDPA applies to "persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that (i) during a calendar year, control or process personal data of at least 100,000 consumers or (ii) control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data." Unlike the CCPA, companies can take solace in the fact that fewer businesses will be subjected to the VCDPA than those that are subject to the CCPA because the

CCPA applies to businesses that have gross annual revenue over \$25 million – which is not limited to revenue generated in California.

Are there any exemptions?

The VCDPA includes exemptions for (1) certain businesses, and (2) types of information and data, which would otherwise be subject to the law's requirements. Such exemptions include:

1. **Business/Entity Exemptions:** Financial institutions or data subject to Title V of the federal Gramm-Leach-Bliley Act are exempted from the VCDPA.
2. **Information and Data Exemptions:** Companies serving clients who are acting in commercial or employment contexts are exempted from the VCDPA. In addition, information and data related to credit reports, as regulated by the federal Fair Credit Reporting Act, and information and data related to vehicle driver information, as regulated by the federal Driver's Privacy Protection Act of 1994, are exempted from the requirements of the law.

What rights are granted to consumers and what does the VCDPA require of businesses?

1. **Consumer Rights:** The VCDPA grants consumers the right to access, correct, delete, obtain a copy of personal data, and opt-out of the processing of personal data. The law further provides that consumers can invoke their rights at any time by submitting a request to the business specifying which rights they want to invoke.
2. **Business Responsibilities:** A company subject to the VCDPA has numerous requirements, including but not limited to:
 - Comply with an authenticated consumer request to exercise any of the rights outlined above within 45 days of receipt of the request, with a grace period of an additional 45 days when reasonably necessary.
 - Establish an appeals process for consumers to use when a company denies a consumer's request to exercise any consumer right.
 - Respond to consumer appeals within 60 days of receipt. If the appeal is denied, companies must provide consumers notice of the denial, as well as provide consumers with an online mechanism (if available), or another method, through which the consumer may contact the Virginia Attorney General's Office (AG) to submit a complaint.

What are the potential penalties?

The AG has exclusive authority to enforce violations of the VCDPA. Companies found to be in violation of the VCDPA are subject to potential injunctions and civil penalties of up to \$7,500 per violation, as well as attorney's fees. It is not clear at this time if state regulators will include a review of VCDPA in their examinations, but businesses should prepare for this possibility and the potential penalties associated with noncompliance.

Further, in contrast to the CCPA, the VCDPA expressly states that consumers do not have a private right of action to sue companies for alleged violations.

What's to come?

Without federal oversight, California and Virginia's enactments of comprehensive consumer data privacy bills signify the emerging policy trend of state oversight and regulation over how companies control and process consumers' personal information. As of April 5, 2021, 14 states have consumer data privacy legislation actively pending in their state legislatures, including: Alabama, Arizona, Colorado, Connecticut, Florida, Illinois, Maryland, Massachusetts, Minnesota, New Jersey, New York, Oklahoma, Texas, and Washington.

As California and Virginia's laws have shown us, we may continue to see states enact *similar*, but not *identical*, laws. The patchwork of varying state privacy laws across the U.S. is likely to continue to spread, state-by-state, until a federal consumer data privacy or protection law or standard is adopted. Until then, the industry should remain vigilant in assessing the applicability of these new state privacy laws and how they will affect their business.