Blogs
March 08, 2021
Virginia Joins California in Adopting a Comprehensive Data Privacy Law

On March 2, 2021, Governor Ralph Northam signed into law Virginia's Consumer Data Protection Act (VCDPA), a comprehensive data privacy law similar to the California Consumer Privacy Act (CCPA). Virginia is now the second state to adopt a comprehensive data privacy law, and many more states are expected to follow suit in the near future. The VCDPA will go into effect on January 1, 2023, the same day that California's new data privacy law, the California Privacy Rights Act (CPRA), goes into effect. Below is an overview of the key provisions of the VCDPA. **Who it applies to:** To be subject to the VCDPA, persons must conduct business in Virginia or produce products or services targeted to Virginia residents and meet one of the following criteria: (1) they control or process personal data of at least 100,000 Virginians during a calendar year; or (2) they control or process personal data of at least 25,000 Virginians and derive over 50 percent of gross revenue from the sale of personal data. **Who it exempts:** The VCDPA exempts five types of entities: (1) Virginia state government entities; (2) financial institutions or data subject to the Gramm-Leach-Bliley Act; (3) covered entities and business associates governed by the U.S. Department of Health and Human Services; (4) nonprofits; and (5) institutions of higher education. **Who it protects:** The VCDPA protects consumers, defined as natural persons who reside in Virginia and act in an individual or household context. The VCDPA, however, does not apply to the personal data of persons acting in a commercial or employment context. Thus, business-to-business and human resources data is outside the scope of the VCDPA. **Party roles:** The VCDPA describes the parties' roles and responsibilities based on whether they are controllers or processors of personal data. A controller is a natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data (i.e., the owner of the data that uses it for its own benefit). A processor is a natural or legal entity that processes personal data on behalf of a controller (i.e., a vendor or service provider). Under the VCDPA, a controller must enter into a binding contract with the processor to govern the processor's data processing procedures, which must include certain requirements described in the VCDPA. Controllers must limit personal data collection to what is "adequate, relevant, and reasonably necessary" for the disclosed purposes; maintain reasonable administrative, technical, and physical data security practices; conduct data protection assessments; obtain affirmative consent before collecting or using sensitive data for any purpose; and not process personal data in a manner that discriminates against consumers. **What data is protected:** The VCDPA protects "personal data," which is broadly defined as any information that is linked or reasonably linkable to an identified or identifiable natural person. Excluded from the definition of personal data is de-identified data and publicly available information, as defined by the statute. The VCDPA also has a separate category of personal data, called "sensitive data," which includes personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status, as well as genetic or biometric data, data relating to children (under the age of 13), and precise geolocation data. Controllers are required to obtain opt-in consent before processing sensitive data. **What data it exempts:** The VCDPA exempts 14 categories of data and information, including data regulated by federal laws such as the Health Insurance Portability and Accountability Act (HIPAA), the Health Care Quality Improvement Act, the Patient Safety and Quality Improvement Act, the Fair Credit Reporting Act, the Driver's Privacy Protection Act, the Family Educational Rights and Privacy Act, and the Farm Credit Act. Human resources data, benefits administration information, and emergency contact data are also exempt. **What rights it provides:** The VCDPA provides Virginians the following data privacy rights: the right to confirmation of processing, the right to correction, the right to deletion, the right to access one's data and to have data portability, and the right to opt out of targeted advertising, sale of personal data, and profiling. Controllers are obligated to honor authenticated consumer requests to exercise these rights within 45 days of receipt of the request. This deadline may be extended by an additional 45 days when reasonably necessary, as long as the controller informs the consumer of the extension within the initial 45-day response period and the reason for the extension. If a controller declines the consumer's request, it must provide its justification and instructions for an appeal. Consumers are entitled to two free requests annually; if requests are unfounded, excessive, or repetitive, the business may charge a reasonable fee to cover the administrative costs

(after the two free requests). **What must be included in your privacy policy:** Controllers are required to include the following in their external-facing privacy policies: (1) the categories of personal data processed; (2) the purpose for processing the personal data; (3) how Virginians can exercise their data privacy rights and appeal a controller's decision to deny a request; (4) the categories of personal data that the controller shares with third parties, if any; (5) the categories of third parties, if any, with whom the controller shares personal data; and (6) whether the controller sells personal data to third parties or processes personal data for targeted advertising. Controllers must describe in the policy at least one secure and reliable means for consumers to submit requests to exercise their consumer rights. **High-risk processing activities:** Under the VCDPA, controllers are required to conduct a data protection assessment if they engage in high-risk processing activities, which include the following: (1) the processing of personal data for targeted advertising; (2) the sale of personal data; (3) the processing of personal data for profiling; (4) the processing of sensitive data; and (5) any other processing activities involving personal data that present a heightened risk of harm to consumers. The controller's data protection assessments are subject to audit by the Virginia Attorney General, as part of a civil investigation demand. **Enforcement and penalties:** The VCDPA does not have a private right of action. The Virginia Attorney General has exclusive authority to enforce the VCDPA but must provide a controller or processor 30 days' written notice to remediate any violations. Failure to comply could expose a controller or processor to civil penalties up to $7,500 for each violation and an injunction. The Attorney General may also recover reasonable expenses incurred in investigating and preparing the enforcement actions, including attorneys' fees. **How to comply with the VCDPA:** To comply with the VCDPA, companies should follow the Six Phases for data privacy compliance, a set of steps formulated based on guidance derived from various data protection sources, including the CNIL (the French Data Protection Authority) and Federal Trade Commission orders, such as the Vizio 2017 order. Companies that are already subject to other comprehensive data privacy laws, such as the CCPA, CPRA, and/or the General Data Protection Regulation, can leverage compliance with these laws to comply with the VCDPA because of the numerous similarities among these laws' provisions. *Guest contributing author Kai Koppoe, CIPP/US, third-year law student at Fordham University School of Law*

## Explore more in

Privacy & Security