Lowenstein Sandler

Privacy & Cybersecurity

March 8, 2021

Virginia Approves New Data Privacy Law: States Take the Lead as U.S. Trends Closer to Europe's GDPR

By Mary J. Hildebrand CIPP/US/E, Edgar R. Hidalgo CIPP/US, and Carly S. Penner CIPP/US

What You Need To Know:

- **Virginia has joined California in adopting a comprehensive data privacy law, with dozens of similar state laws pending.**
- **In the absence of federal legislation, businesses must comply with different data protection requirements on a state-by-state basis.**
- **Organizations that seek to retain a competitive edge and avoid regulatory and legal entanglements would be well-advised to accelerate–or begin–compliance efforts now.**

On March 2, the Virginia Consumer Data Protection Act (VCDPA) was signed into law, becoming the second comprehensive state privacy law in the United States. The VCDPA reflects core principles from the California Consumer Privacy Act of 2018 (CCPA) and its progeny, the California Consumer Rights Act (CPRA), adopted in 2020. However, the VCDPA departs from its West Coast predecessors in certain key respects and illustrates a growing trend of U.S. data privacy laws moving closer to the European General Data Protection Regulation (GDPR).

To whom does the VCDPA apply?

The VCDPA applies to any company conducting business in Virginia or targeting its products and services to Virginia residents that:

- Controls or processes the personal data of at least 100,000 Virginia residents in a calendar year; or
- Controls or processes the personal data of at least 25,000 Virginia residents and derives more than 50 percent of its gross revenue from the sale of personal data.

In a departure from the California laws, the VCDPA explicitly carves out financial institutions regulated by the Gramm-Leach-Bliley Act (GLBA), as well as covered entities and business associates subject to the Health Insurance Portability and Accountability Act (HIPAA). California adopted a more surgical approach by exempting *data* regulated by GLBA and HIPAA but not the organizations themselves.

What type of data does the VCDPA protect?

The VCDPA protects the personal data of residents of Virginia. Like the CPRA and the GDPR, the VCDPA divides personal data into two broad categories: personal data and sensitive data. Personal data includes any information that is linked or reasonably associated to an identified or identifiable natural person. Sensitive data is personal data that reveal (i) racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; (ii) genetic or biometric data processed for the purpose of uniquely identifying a natural person; (iii) personal data collected from a known child; or (iv) precise geolocation data. Additionally (and

likely taking a cue from the post-enactment moratoria on enforcement under the CCPA), the VCDPA explicitly exempts B2B business contact data and the personal data of employees.

What does the VCDPA require?

Privacy disclosures. Like the California laws, controllers are required to establish privacy policies that include disclosures about use of personal data and consumer rights. Additionally, both the California laws and the VCDPA have requirements to maintain "reasonable" security measures.

Opt-in consent may be required. Unlike the California laws, under the VCDPA, businesses are required to obtain consent to process sensitive data. Notably, this opt-in requirement aligns the VCDPA with the GDPR on the collection of sensitive data.

"Sale" clarified, but other opt-out rights added. Like the California laws, the VCDPA grants Virginia consumers the right to opt out of the sale of their personal data. Under the VCPDA however, "sale" only applies to the exchange of personal data for monetary consideration. This is a welcome departure from the far broader concept of "sale" under the California laws. Despite narrowing the scope of the sale opt-out right, the VCDPA grants Virginia consumers additional opt-out rights specifically related to targeted online advertising and profiling.

Processor contractual requirements. Similar to new provisions in the CPRA, the VCDPA requires businesses to flow down certain contractual obligations to their vendors and other third parties who process personal data on their behalf. This requirement aligns the California privacy regime and the VCDPA closer to the Article 28 standards under the GDPR.

Data protection assessments. Similar to the CPRA, the VCDPA introduces the requirement to conduct periodic data protection risk assessments when processing sensitive data or when engaging in targeted advertising, selling of personal data, profiling, and other activities of heightened risk to consumers. These risk assessment requirements are yet another concept borrowed from the GDPR.

What are the key takeaways?

The VCDPA became effective immediately with an enforcement date of January 1, 2023, which aligns with the start date for enforcement under the CPRA. As many U.S. businesses that have addressed GDPR and CCPA compliance can testify, Virginia legislators have not provided a generous grace period. Regulated businesses should not underestimate the time necessary to achieve compliance. Additionally, we are likely to see a deluge of state legislative activity in privacy this year. Other U.S. states will likely pass their own data protection laws which will need to be integrated into comprehensive privacy programs and business operations. On March 3, the Washington state Senate passed Senate Bill 5062 (labeled the Washington Privacy Act) by a nearly unanimous margin. And many other states, including New York and Florida, have introduced (in some cases reintroduced) CCPA-like privacy legislation. CCPA-compliant organizations need to revisit the policies, processes, and procedures already implemented and revise them to comply with the VCDPA, the CPRA, and other regimes in the legislative pipeline. And organizations that have not yet addressed privacy compliance will need to start comprehensive compliance efforts from the ground up. As pending privacy legislation progresses, we will continue to provide updates through our client alerts.

About Us

In today's digital world, where data has become a key asset for conducting business, companies continue to face greater privacy and cybersecurity challenges. At Lowenstein Sandler, our Privacy & Cybersecurity team helps clients navigate the rapidly evolving, increasingly complex privacy and security law landscape in the United States, the EU, and around the world. We deliver innovative privacy and security solutions that meet our clients' critical business needs including the commercialization of data assets in a legally compliant manner. Our targeted counsel is relevant to companies across diverse industry sectors, and public and private companies from start-ups to global enterprises.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

MARY J. HILDEBRAND CIPP/US/E
Partner
Chair, Privacy & Cybersecurity
T: 973.597.6308
mhildebrand@lowenstein.com

EDGAR R. HIDALGO CIPP/US
Counsel
T: 973.422.6418
ehidalgo@lowenstein.com

CARLY S. PENNER CIPP/US
Associate
T: 973.597.2516
cpenner@lowenstein.com