Next Up: Virginia Slated to be Second State to Enact Comprehensive Data Privacy Law

On Feb. 5, 2021 the Virginia State Senate unanimously approved Senate Bill 1392, titled the Virginia Consumer Data Protection Act (VCDPA). The Virginia House of Delegates previously approved identical companion legislation and the reconciled bill was signed into law by the governor on March 2, 2021.

Virginia is now the second state to pass major data privacy legislation following in the footsteps of California. The California Consumer Privacy Act (CCPA) was enacted in 2018 and was recently revised by Proposition 24 (California Privacy Rights Act- CPRA). Like the European Union General Data Protection Regulation (GDPR) and CCPA/CPRA, the Virginia law establishes a comprehensive framework concerning the controlling and processing of Virginia residents' personal data. The law will become effective Jan. 1, 2023. Some of the most important aspects of the law are detailed below.

What Does VCDPA Do?

The VCDPA expands consumer rights to access, delete, correct and obtain a copy of personal data provided to or collected by covered entities. In addition, it provides for opt-out rights of the processing of personal data including targeted advertising, sale or profiling. Like GDPR and CCPA/CPRA, Virginia included in its definition of personal data "sensitive data," which covers data such as race, religion, sexual orientation and biometric data. To process sensitive data, controllers will need affirmative consent from consumers. The law includes a very high standard for what constitutes affirmative consent, similar to the definition under GDPR.

Data controllers are subject to many requirements that are also seen under GDPR and CCPA/CPRA. For example, data controllers must not collect more personal data than is necessary for their data processing purposes, implement reasonable security measures, limit the processing to what was disclosed to consumers, and refrain from discriminating against consumers that exercise their rights. The law also requires increased transparency between controller and consumer. Such transparency includes privacy notices and instructions on how consumers can opt-out of having their data processed. Lastly, like under GDPR, controllers must conduct and document a privacy risk assessment when they process data that is at high risk to result in consumer harm.

Who does the law apply to?

Unlike the laws in California, the Virginia law does not set a revenue threshold. The law applies to 1) businesses that control or process data for at least 100,000 Virginia residents; or 2) businesses that make 50% or more of their gross revenues from the sale of personal data and control or process data of at least 25,000 Virginia residents. The lack of revenue threshold may result in many small and medium sized businesses being outside the scope of the law.

Notably, the law does not apply to institutions of higher education, Virginia state agencies, nonprofits or entities covered by another data privacy regulatory scheme.

What are the enforcement mechanisms?

The attorney general has exclusive jurisdiction to enforce the VCDPA. The Virginia law does not include a private right of action. This is in stark contrast to California, that just expanded private rights of action under CPRA. This was a point of contention among Virginia lawmakers, concerned that the attorney general would not have enough resources for enforcement. However, the law includes funds to start a new office under the Attorney General to enforce compliance with VCDPA.

What does this mean for your business?

Virginia's legislation is likely just the beginning of a national trend for state specific data privacy legislation. Companies that do business in multiple states will want to ensure compliance with each state's laws, and should not overlook the differences among them. Specifically, businesses subject to VCDPA will want to work on compliance efforts now to ensure adequacy when the law becomes effective.

For more information regarding the Virginia Consumer Data Protection Act and compliance efforts businesses should be taking, contact Amber Lawyer, Shannon Knapp or any attorney in the Cybersecurity and Data Privacy practice.

BOND SCHOENECK & KING ATTORNEYS