

Virginia Contemplates Sweeping New Data Protection Law

Privacy, Cyber & AI Decoded Alert | 3 min read

Feb 4, 2021

** Update, March 2, 2021: Governor Ralph Northam today signed the Customer Data Protection Act into law, making Virginia the second state in the nation to pass a comprehensive privacy regulation after California. The Act goes into effect on January 1, 2023.*

** Update, February 5, 2021: Senate Bill 1392 has been passed in the Virginia Senate. As noted, an identical companion bill previously was passed by the House of Delegates. If Governor Northam signs off, the Virginia Consumer Data Protection Act will go into effect on January 1, 2023.*

A [comprehensive data protection and privacy bill](#), titled the Consumer Data Protection Act, has been introduced in the Virginia state senate. With notable exceptions the proposal contains privacy and cybersecurity provisions similar to those contained in the California Consumer Privacy Act, the California Privacy Rights Act, and the E.U.'s General Data Protection Regulation.

The bill would create a number of personal data rights for consumers. Under the bill, “consumer” is defined as “a natural person who is a resident of the Commonwealth acting only in an individual or household context,” excluding persons “acting in a commercial or employment context.” Personal data means “any information that is linked or reasonably linkable to an identified or identifiable person.”

The proposed law would give consumers the right to:

- Confirm whether or not a controller is processing the consumer’s personal data;
- Correct inaccuracies;
- Delete personal data; and
- Opt-out of processing of personal data for:
 - targeted advertising;
 - sale of personal data; or
 - profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

Among other obligations, data controllers would be required to:

- Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which it is processed, as disclosed to the consumer;
- Not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;
- Not process "sensitive data" – which includes biometric and genetic data, data revealing racial or ethnic origin, mental or physical health diagnosis, sexual orientation, personal data collected from a known child, and precise geolocation data – without consent; and
- Provide a reasonably accessible, clear, and meaningful privacy notice that includes:
 - The categories of personal data processed;
 - The purpose for processing;
 - How consumers may exercise their rights;
 - The categories of personal data shared with third parties; and
 - The categories of third parties with whom personal data is shared.

Controllers also would be required to implement "reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data" and to conduct and document a "data processing assessment" for certain types of processing activities, including the processing of personal data for targeting advertising, the sale of personal data, and the processing of sensitive data.

Importantly, unlike California law, there is no private right of action in the proposed Virginia law; only the Attorney General would be empowered bring an enforcement action. The bill provides for a 30 day cure period for violations identified by the Attorney General. Continuing violations would be subject to maximum damages of \$7,500 per violation, as well as a civil penalty up to \$7,500 per violation, in a civil action brought by the Attorney General. All collected civil penalties would be paid into a new Consumer Privacy Fund, which would be used to support the Attorney General's enforcement work.

The bill has moved through the Senate Committee on General Laws and Technology and was referred to the Senate Finance Committee on January 27, 2021. A [companion bill](#) was passed in the House of Delegates on January 29, 2021. If enacted, the law would go into effect on January 1, 2023.

Related Capabilities

Data Privacy, AI & Cybersecurity