

Virginia Passes Broad Data Privacy Law

MARCH 3, 2021

On March 2, 2021, Virginia Governor Ralph Northam signed the [Virginia Consumer Data Protection Act](#) (CDPA) into law, setting up the newest state to enact broad privacy legislation aimed at giving consumers more control over their personal data. The bill will go into effect on January 1, 2023.

Once in effect, the CDPA, which does not contain a set revenue threshold, will apply to all persons that conduct business in Virginia and either (i) control or process data for at least 100,000 Virginians or (ii) that make 50% of their gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers. Like the CCPA, the CDPA defines “personal information” broadly to include “any information that is linked or reasonably linkable to an identified or identifiable person,” with exceptions for certain types of data governed by federal law. However, unlike the CCPA, a “sale” under the CDPA is limited to exchanges of personal data for *monetary* consideration.

The CDPA will impose several changes in the handling of Virginia consumer data. Specifically, the CDPA gives Virginians the right to correct inaccuracies, the right to delete their personal data, and the right to know the information being processed or sold by the business about them. Notably, the CDPA also gives Virginia consumers the right to opt-out of the processing of their personal data for targeted advertising, sales, or profiling in furtherance of decisions with legally significant effects concerning the consumer. Under the CDPA, “targeted advertising” does not include ads that are solely based on information obtained from the consumer’s visit to the organization’s website. However, if an organization processes personal data for targeted advertising, it must disclose such processing and, in a clear and conspicuous manner, disclose how consumers may submit a verifiable request objecting to such processing. When a consumer objects to the processing of their personal data for targeted advertising, the controller must no longer process the personal data for that purpose and must take reasonable steps to communicate the consumer’s objection to any third parties with whom the controller sold the consumer’s personal data for that purpose.

In addition to the consumer rights granted under the CDPA, the bill also imposes several new obligations on data controllers like the requirements recently passed in the California Privacy Rights Act (CPRA). First, data controllers must limit the collection of personal data to only what is adequate, relevant, and reasonably necessary for the purpose of the processing. Data controllers are also prohibited from processing “sensitive data,” including biometric or geolocation data, or data revealing racial or ethnic origin or sexual orientation, without consent from the

consumer. Under the CDPA, data controllers must provide a reasonably accessible and clear privacy notice describing how the organization collects, processes, and shares personal information.

Additionally, the CDPA imposes additional data security requirements on data controllers. Under the CDPA, data controllers must 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 protection assessment for certain types of processing activities, including the processing of personal data for targeted advertising, the sale of personal data, and the processing of sensitive data.

Unlike the CCPA, the CDPA does not allow for a private right of action for consumers. Instead, the Virginia Attorney General has the exclusive right to bring enforcement actions against organizations. The CDPA allows for a 30-day cure period for any CDPA violations identified by the Attorney General, with continuing violations 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. The CDPA also contemplates a Consumer Privacy Fund that will primarily be used to fund the Attorney General’s enforcement work and may be used to provide monetary compensation to individual consumers.

TIP: Companies should assess how they collect, use, and share personal information. This knowledge will enable companies to quickly assess whether the CDPA and future state privacy laws will apply to their organization and will aid in updating business practices to comply with the new privacy law requirements.

3 Min Read

Author

[Eric Shinabarger](#)

Related Locations

Chicago

Los Angeles

San Francisco

Silicon Valley

Washington, DC

Related Topics

CCPA

CDPA

CPRA

Related Capabilities

Privacy & Data Security

Compliance Programs

Related Regions

North America

Related Professionals



Eric Shinabarger

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.