wiley

ALERT

Virginia Enacts Comprehensive Privacy Legislation

March 4, 2021

Earlier this week, the Commonwealth of Virginia became the second state to enact comprehensive consumer data privacy legislation, joining California. On March 2, Governor Ralph Northam signed the Consumer Data Protection Act (CDPA) into law, as he was widely expected to do. The CDPA garnered widespread support in Virginia's House and Senate and was pushed across the goal line in Richmond relatively quickly.

The CDPA establishes a framework for controlling and processing personal data in Virginia. At a high level, it:

1. Applies to an entity or individual that conducts business in Virginia or targets their products or services to Virginia residents and that meets minimum thresholds for controlling and processing (or selling) personal data;
2. Establishes key consumer rights, including the right to access personal data, the right to correct inaccurate personal data, the right to delete personal data, the right to obtain a copy of personal data, and the right to opt-out from sales of personal data, targeted advertising, and certain profiling;
3. Imposes a number of obligations on controllers, including data minimization and security obligations, a requirement to obtain consent before processing "sensitive data," and a requirement to conduct data protection assessments under certain circumstances; and
4. Requires that Virginia's Joint Commission on Technology and Science create a work group comprised of key government officials, representatives of businesses covered by the law, and consumer rights advocates to assess the implementation

Authors

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Kyle M. Gutierrez
Associate
202.719.3453
kgutierrez@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

State Privacy Laws

of the CDPA and release a report on its findings by November 1, 2021.

The CDPA will become effective on January 1, 2023. While there are similarities between the CDPA and California's framework, the two approaches are distinct, so companies that are governed by both will need to consider how to develop a compliance plan that is interoperable. We provide a more in-depth analysis of the CDPA below:

The CDPA's Scope

The CDPA applies to an entity (or individual) that conducts business in Virginia or targets their products or services to Virginia residents and (i) "control[s] or process[es] personal data of at least 100,000 consumers" over the course of a calendar year or (ii) "control[s] or process[es] personal data of at least 25,000 consumers and derive[s] over 50 percent of gross revenue from the sale of personal data" (Data Controller). The CDPA does not apply to state or local governmental entities, nonprofit organizations, higher learning institutions, or entities covered by the Gramm-Leach-Bliley Act, HIPAA, or the HITECH Act, and does not cover certain types of personal data already protected under federal law.

Consumer Rights Provided by the CDPA

The CDPA grants consumers five personal data rights, which consumers may invoke by submitting a request to a Data Controller: (1) the right to confirm whether a controller is processing the consumer's data and, if so, to access that data; (2) the right to correct inaccuracies in the consumer's personal data; (3) the right to have the consumer's personal data deleted; (4) the right to obtain a copy of the consumer's personal data; and (5) the right to opt out of the processing of the consumer's personal data for purposes of targeted advertising, selling that data, or profiling in order to make impactful decisions.

In this sense, the CDPA largely parallels the California Consumer Privacy Act (CCPA), which also provides California consumers with the right to know what personal data a business has collected from them and whether that data is being sold or disclosed, the right to prevent the sale of the consumer's personal data, and the right to access the consumer's personal data, among other things. It goes further than the current CCPA in some ways. For example, it extends the opt-out right to cover certain types of data processing, for targeted advertising, and some profiling.

Obligations Imposed on Data Controllers Under the CDPA

Under the CDPA, Data Controllers are subject to several general obligations. Specifically, Data Controllers must: (1) collect no more personal data than is necessary for their data processing purposes; (2) only process personal data for the purposes that they have disclosed to consumers; (3) implement reasonable data security measures; (4) refrain from discriminating against consumers that exercise their personal data rights; and (5) obtain a consumer's consent before processing "sensitive data" – which the CDPA defines to include a consumer's racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship status, genetic or biometric data, personal data collected from a child, and precise geolocation data.

Beyond these general obligations, the CDPA also requires that controllers take several steps to increase transparency with consumers, like providing a clear and meaningful privacy notice and disclosing whether the controller sells personal data to third parties or processes personal data for purposes of targeted advertising. Controllers must also disclose how consumers can opt out of having their data used like this. Additionally, controllers must conduct and document a privacy risk assessment when they process data for certain purposes that pose a "heightened risk" of consumer harm.

Enforcement of the CDPA

The CDPA explicitly declines to create a private right of action to enforce these rights. Rather, the authority to enforce the CDPA is vested solely with the Commonwealth's Attorney General.

In terms of penalties, controllers or processors of personal data that violate the CDPA could be subject to an injunction and liable for up to $7,500 per violation. The CDPA also establishes a "Consumer Privacy Fund," into which all civil penalties collected for violations of the CDPA will be deposited in order to fund the Attorney General's further enforcement efforts.

Looking Forward

Starting January 1, 2023, Data Controllers that conduct business in the Commonwealth will find themselves subject to several important obligations, so it is vital that businesses that will be covered by the CDPA begin to determine how they will bring themselves into compliance with the law by then. At the same time, businesses subject to the CDPA also must consider other potentially applicable state laws, such as the California Privacy Rights Act, and begin mapping out privacy compliance strategies accordingly.

Wiley's Privacy, Cyber & Data Governance Team has helped entities of all sizes from various sectors proactively address risks and address compliance with new privacy laws. Please reach out to any of the authors with questions.