**David J. Kappos**
+ 1-212-474-1168
dkappos@cravath.com

**Richard J. Stark**
+1-212-474-1564
rstark@cravath.com

**David M. Stuart**
+1-212-474-1519
dstuart@cravath.com

**Evan Norris**
+1-212-474-1524
enorris@cravath.com

# Virginia Enacts the Consumer Data Protection Act

*March 10, 2021*

On March 2, 2021, the Governor of Virginia signed into law the Virginia Consumer Data Protection Act (the "CDPA"). The CDPA, which goes into effect on January 1, 2023, imposes broad new obligations on businesses in their capacity as controllers and processors of personal data, including data security requirements. The CDPA also grants consumers a number of new rights over their personal data that give rise to additional obligations on businesses. Virginia is now the second U.S. state, after California, to have enacted a comprehensive data privacy and protection regime. While the CDPA differs in a number of important respects from the California Consumer Privacy Act ("CCPA") —including in that it does not create a private right of action— its enactment represents a significant development in the U.S. regulatory landscape.

## SCOPE

### What businesses are subject to the CDPA?

The CDPA applies broadly to entities that (i) conduct business in Virginia or (ii) produce products or services that are targeted to Virginia residents, *and* (iii) meet one of the following criteria:

- annually control or process personal data of at least 100,000 consumers; *or*
- control or process personal data of at least 25,000 consumers and derive over 50% of gross revenue from the sale of personal data.

Notably, the CDPA lacks a standalone revenue threshold-in contrast to California's law, which applies to businesses with more than $25 million in gross annual revenue.

The CDPA protects "personal data" of "consumer[s]", defined as information that is "linked or reasonably linkable to an identified or identifiable natural person" who is also a resident of Virginia. Among other things, these definitions exclude publicly available information, as well as data collected in a "commercial or employment context" (as opposed to an "individual or household context"). The latter is particularly noteworthy as it effectively exempts all employee personal data and other personal data collected in the employment and business-to-business context from the reach of the new law.

Adopting the core concepts introduced by the European Union's General Data Protection Regulation ("GDPR"), the CDPA distinguishes between businesses that are "controllers" of personal data, which determine what data to collect and what to do with it, and those that are "processors" of personal data, *i.e.*, the service providers that process data on behalf of controllers. Both controllers and processors are covered businesses under the CDPA, but, as described below, Virginia's new law imposes differing obligations on the basis of this distinction.

In addition to the types of data discussed above, the CDPA exempts, among other entities and data, colleges and universities, nonprofit organizations, financial

institutions and data "subject to" regulation under Title V of the Gramm-Leach-Bliley Act, covered entities and business associates "governed by" by the privacy, security and breach notification rules under the Health Insurance Accountability and Portability Act ("HIPAA"), and public health information under HIPAA.

#### What obligations does the CDPA impose on businesses?

The CDPA imposes a number of obligations on businesses, depending on whether the business is a controller or a processor. Controllers must provide a privacy notice that establishes, among other things, the purpose for processing personal data. Controllers can only process personal data without consumers' consent if such processing is reasonably necessary to or compatible with the purpose as disclosed to consumers. Relatedly, controllers must limit their collection of personal data to such data that is "adequate, relevant, and reasonably necessary" for processing, according to the disclosed purpose. In addition, controllers are prohibited from processing "sensitive data", defined as personal data that reveals, among other things, race, religious beliefs, health diagnoses, sexual orientation, or citizenship or immigration status, without the consumer's consent. Controllers also cannot process personal data in violation of state and federal discrimination laws or discriminate against a consumer for exercising the consumer rights conferred by the CDPA (discussed in more detail below), including by denying goods to the consumer.

In addition, the CDPA imposes data security obligations on controllers, including a mandate that they "establish, implement and maintain reasonable administrative, technical, and physical data security practices" to protect personal data. What this means from controller to controller will vary, as the CDPA requires that a controller's practices be "appropriate to the volume and nature of the personal data at issue". Notably, the CDPA also requires that controllers conduct and document a data protection assessment that evaluates various processing activities, including the sale of personal data, processing of personal data for targeted advertising, processing of sensitive data and any personal data processing activities that present a heightened risk of harm to consumers. This data protection assessment must weigh the risks and benefits associated with processing consumers' personal data, as mitigated by the safeguards employed by the controller to reduce associated risks. Controllers must disclose the results of any assessment to the Virginia Attorney General upon request, but the assessments are otherwise confidential.

Processors also have a number of obligations under the CDPA. Among these are the obligation to assist controllers in implementing the CDPA's data security measures, including the performance of the data protection assessment, and adhering to the data breach notification requirements under Virginia's data breach notification law (Va. Code § 18.2-186.6). In addition, the CDPA requires that processors and controllers enter into contracts that clearly define instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties.

#### What rights does the CDPA grant to consumers?

The CDPA grants consumers broad rights with respect to businesses' use of their personal data. These consumer rights parallel the new and expanded rights of the California Privacy Rights Act-enacted by ballot measure last November-which amends the CCPA effective January 1, 2023. Under Virginia's new law, a consumer has the right to request that a controller:

- confirm whether it processes the consumer's personal data and provide access to any such data;
- correct inaccuracies in the consumer's personal data;
- delete personal data provided by or obtained about the consumer;
- provide a copy of the consumer's personal data in a readily usable and transmittable format; and
- permit the consumer to opt out of the processing of personal data for purposes of targeted advertising, sales or "profiling in furtherance of decisions that produce legal or similarly significant effects".

The CDPA imposes a corresponding obligation on controllers to respond to a consumer's rights request and to establish and conspicuously make available an appeals process when such requests are denied. If an appeal is denied, the controller must further provide a method by which the consumer may submit a complaint to the Virginia Attorney General.

## ENFORCEMENT

The Virginia Attorney General is granted exclusive authority to bring enforcement actions for violations of the CDPA on behalf of affected consumers. Upon the law's effective date, the Attorney General will be authorized to issue civil investigative demands to any controller or processor believed to be engaged in, or about to engage in, any violation. The Attorney General may seek injunctive relief or statutory damages of up to $7,500 for each violation, but only after first providing 30 days' written notice and identifying the specific provisions of the CDPA alleged to have been violated. If the controller or processor cures the alleged violation within the 30-day period and provides express written notice of that fact, then no enforcement action can be initiated to recover damages for the alleged violation. By contrast, California's new law will remove the CCPA's current 30-day cure period for public enforcement actions once it takes effect in 2023. And unlike both California's current and new laws, which include private enforcement provisions, the CDPA expressly states that it does not create a private right of action.

## CONCLUSION

Virginia joins California as one of two U.S. states to enact a comprehensive data privacy and protection regime. As we watch to see if more states follow suit–and indeed if Congress ultimately enacts a uniform nationwide framework–it is not too early for businesses to consider bringing themselves into compliance with the CDPA (as well as the California Privacy Rights Act, which also comes into effect on January 1, 2023). Among other things, we encourage businesses within and outside of Virginia to (i) review whether they fall within the CDPA's jurisdictional thresholds and, if warranted, (ii) conduct a preliminary data protection assessment of the type contemplated by the new law and (iii) otherwise evaluate and begin to address any gaps between their existing privacy policies (whether designed to achieve compliance with the CCPA, GDPR and/or other applicable regimes) and the new obligations the CDPA will soon impose.



**New York**
Worldwide Plaza
825 Eighth Avenue
New York, NY 10019-7475
+1-212-474-1000

**London**
CityPoint
One Ropemaker Street
London EC2Y 9HR
+44-20-7453-1000

www.cravath.com