

Virginia Governor Signs Consumer Data Protection Act into Law



March 29, 2021

Virginia Governor Signs Consumer Data Protection Act into Law

On March 2, 2021, Virginia Governor Ralph Northam signed the Virginia Consumer Data Protection Act (“VCDPA”) into law. Virginia is the second state to enact a comprehensive privacy statute, following California’s enactment of the Consumer Privacy Act (“CCPA”), which is entering its second year of effectiveness, and the Privacy Rights Act (“CPRA”). The VCDPA will take effect on January 1, 2023, the same effective date as the CPRA.

As the first comprehensive privacy law passed through a traditional legislative process without pressure from a popular ballot initiative, proponents of the VCDPA pitched the statute as an “omnibus bill” that “holds companies accountable for protecting consumer data in providing protections for consumers.”¹ The privacy regime created by the VCDPA draws heavily from laws and regulations in effect, such as the CCPA, and CPRA, and the European Union General Data Protection Regulation 2016/679 (“GDPR”), and from proposed legislation such as the Washington Privacy Act. The provisions of the VCDPA outline responsibilities and privacy protection standards for both “data controllers” and “processors,” borrowing those terms from the GDPR. However, there are also significant differences between the VCDPA and existing data protection regimes. For example, the VCDPA includes a requirement that organizations conduct data protection assessments and implement certain policies and procedures to ensure compliance. Additionally, because the VCDPA includes broad exemptions from coverage for both certain classes of entities and enumerated types of data already covered by federal data protection laws, it may affect a more limited group of companies and organizations than the CCPA or the GDPR.

Organizations will need to carefully assess whether their activities are covered by the VCDPA, and if they are, take steps to ensure they comply with it by 2023. The law applies to both U.S. and non-U.S. companies that process personal information of over 100,000 Virginia consumers, or that process information of over 25,000 Virginia consumers and also derive more than 50% of their revenue from the sale of this data.

This alert summarizes the VCDPA’s scope and applicability, the obligations it imposes on data controllers and processors, the rights it grants to consumers, its rules governing sensitive information, and the enforcement regime it implements. We also compare the VCDPA with other comprehensive data privacy regimes such as the CCPA and the GDPR, highlighting key similarities and differences. Finally, we discuss potential implications of the VCDPA—including whether the statute may presage further developments in

¹ Comment of Sponsor Sen. David Marsden (D-Fairfax) - <https://www.virginiabusiness.com/article/va-set-to-become-2nd-state-with-consumer-data-protection-law/>

state and federal privacy laws in the United States—and discuss whether companies’ existing compliance approaches may need to be adjusted to comply with the VCDPA.

Key Provisions of the VCDPA

Applicability: Covered Entities and Information

The VCDPA covers “persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth” and that meet either of the following jurisdictional thresholds:²

- Annually control or process personal data of at least 100,000 Virginia residents; or
- Control or process personal data of at least 25,000 Virginia residents and derive over 50% of gross revenue from the sale of personal data.

The VCDPA’s definitions of various types of data and “covered individuals” further clarify its scope:³

- “Personal data” is defined similarly to the GDPR, as “any information that is linked or reasonably linkable to an identified or identifiable natural person.” This definition excludes de-identified data, and may differ from the CCPA and CPRA by potentially excluding data that can only be associated with households, and not particular individuals.⁴
- “Sensitive data” is defined separately from the definition of “personal information” to include, among other data, personal data revealing racial or ethnic origin, data collected from children, and precise geolocation data. This follows the approach taken by the CCPA/CPRA, as well as Article 9 of the GDPR. However, unlike either the CCPA/CPRA or the GDPR, the VCDPA imposes additional requirements on controllers and processors to secure affirmative consumer consent prior to collecting any such information.

² Va. Code. Ann. § 59.1-572(A).

³ *Id.* at § 59.1-571.

⁴ The provisions of the VCDPA indicating that it applies to individuals acting in a household context is in tension with provisions that appear to exclude data associated only with households and not individuals. These provisions make it unclear whether the provisions of the VCDPA apply to information such as IP addresses, which may be associated with both households and individuals.

Further limiting the scope of the statute's applicability, the VCDPA does not apply to individuals in commercial and employment contexts, and is limited to Virginia residents "acting only in an individual or household context."⁵

Exemptions

The VCDPA also exempts certain types of entities and certain types of data from its requirements:⁶

- Exempted entities include government entities, nonprofits, institutions of higher education, and organizations subject to other data privacy regimes such as the Health Insurance Portability and Accountability Act ("HIPAA") and the Gramm-Leach-Bliley Act ("GLBA"), among others.
- Similarly, personal data governed by enumerated federal data protection regulations, including financial information under the GLBA and certain personal health information under the HIPAA, is exempted from the statute.
- Data collected on individuals acting in a commercial or employment context is also exempt from the coverage of the statute, meaning that controlling or processing personal data in the business-to-business context, or as an employer, does not fall within the scope of the VCDPA.

Consumer Rights

Covered Virginia consumers are granted broad rights with respect to their personal data under the VCDPA. These include the right to access, correct, delete, and obtain their data in a portable format, and to opt out of the processing of personal data for purposes including targeted advertising, sale, or profiling in certain contexts. Consumers also have the right to appeal a business's denial of a data request "within a reasonable time after the consumer's receipt of the decision." If the appeal is denied, the controller must further inform the consumer about how to submit a complaint to the attorney general if he or she so chooses.⁷

Unlike the CCPA or CPRA, consumers in Virginia cannot delegate their rights to authorized agents, and must exercise these rights individually. The VCDPA also only permits individuals to opt out of processing of their personal data for the three specific purposes described above, unlike the broader opt-outs provided under the California regime.⁸

⁵ *Id.* at § 59.1-571.

⁶ *Id.* at § 59.1-572(B)-(C).

⁷ *Id.* at § 59.1-573.

⁸ *Id.* at § 59.1-573(A)(5)

Obligations of Data Controllers and Processors

Under the VCDPA, data controllers have a duty to limit their collection of personal data to that which is “adequate, relevant, and reasonably necessary” to fulfill the purposes disclosed to consumers. This language is similar to the Article 6 requirements under the GDPR, which require processing of personal data to be “necessary” for specific purposes or settings.⁹

Data controllers are also required to (1) provide a privacy policy with specific provisions enumerated in § 59.1-574(C); (2) respond to consumer rights requests within a specified time period¹⁰; and (3) establish and implement reasonable data security practices to protect personal data.¹¹

Additionally, the VCDPA requires controllers to ensure that any de-identified data, defined as “data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such a person,” cannot be re-identified. Accordingly, controllers of de-identified data, or pseudonymous data—defined as “personal data that cannot be attributed to a specific natural person without the use of additional information”—are exempted in certain contexts from complying with access, deletion, correction, or portability requests from consumers if there is a risk that doing so may re-identify the data or associate it with any natural person.¹²

Importantly, the new Virginia statute also requires businesses that engage in certain processing activities involving personal data to conduct a data protection assessment (“DPA”). The DPA is similar to the Data Protection Impact Assessment (“DPIAs”) required by Art. 35 of the GDPR, although the VCDPA requires DPAs under different circumstances. DPAs require businesses to conduct a cost-benefit risk assessment for certain processing activities, and they can be reviewed during any investigation by the Attorney General.¹³

The VCDPA’s provisions regarding data processors—defined as entities that process personal data on behalf of a controller—generally require processors to conduct processing activities according to the instructions of controllers. Similar to the requirement for Data Processing Agreements between data controllers and processors under the GDPR, the VCDPA requires written contracts between any controller, processor, and sub-processor before any party begins processing personal data covered by the statute.

⁹ *Id.* at § 59.1-575.

¹⁰ *Id.* at § 59.1-573(B)(1).

¹¹ *Id.* at § 59.1-574(A)(3).

¹² *Id.* at § 59.1-571; § 59.1-577.

¹³ *Id.* at § 59.1-576.

Treatment of Sensitive Personal Information: “Opt-In Required”

In separately defining more sensitive types of personal information, the VCDPA follows the model of both the CCPA/CPRA as well as the GDPR. “Sensitive Personal Information” is defined to include:¹⁴

- Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;
- The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;
- The personal data collected from a known child; and
- Precise geolocation data.

The VCDPA further draws from the GDPR by mandating that covered companies obtain opt-in consent to collect or process sensitive data. Entities dealing with sensitive personal information must first obtain a “clear affirmative act signifying a consumer’s freely given, specific, informed, and unambiguous agreement” to the processing. The Virginia statute thus creates the first opt-in privacy regime of any comprehensive privacy law in the U.S.¹⁵

Enforcement

The Virginia statute provides for enforcement solely by the Virginia Attorney General (“AG”). Although the penalty per violation is identical to that set out by the CCPA, the Virginia statute contains no equivalent private right of action.

To inform investigations, the Virginia AG may compel production of any DPAs conducted by data controllers or processors without court approval. The VCDPA also requires that the AG provide “30 days’ written notice” to the subject of any alleged current or past violation to provide them with an opportunity to cure the violation. If a controller fails to cure the alleged violation, the AG may issue fines of up to \$7,500 per violation. These fines would go towards a “consumer privacy fund” that may be used to ensure minimum levels of enforcement by the AG.¹⁶

¹⁴ *Id.* at § 59.1-571.

¹⁵ *Id.* at § 59.1-571.

¹⁶ *Id.* at § 59.1-580.

Comparison with other Comprehensive Privacy Regimes

How the VCDPA Compares to California's Data Privacy Laws

The VCDPA may apply more broadly in some instances than the CCPA/CPRA, and more narrowly in others. The Virginia statute may apply more broadly than the CCPA because it uses a more inclusive definition of “doing business” that captures not only entities that conduct business in Virginia, but also entities that “produce products or services that are targeted to residents of the Commonwealth.”¹⁷

However, the VCDPA may be less inclusive than the CCPA because it does not include a revenue threshold that automatically subjects companies of a certain size doing business in the state to obligations under the statute. Accordingly, even large businesses doing business in Virginia may not be subject to the law if they do not control or process data from more than 100,000 Virginia consumers (or 25,000 Virginia consumers if they also derive over 50% of their revenues from the sale of such data). Additionally, the VCDPA restricts what may qualify as the “sale of data” to “the exchange of personal data for monetary consideration.”¹⁸ In contrast, the CCPA defines essentially any exchange of consideration as a “sale.”

The exemptions concerning types of data under the VCDPA also are significantly more expansive than the CCPA's exemptions, as they permanently exempt personal information gathered in the employment and B2B settings. Unlike the CCPA's similar exemptions, there is no sunset to these exemptions, so data collected on individuals in an employment or commercial context is fully exempt under the VCDPA. Furthermore, there is no equivalent under the Virginia regime to the CCPA's requirement that businesses that collect personal information in employment or B2B settings provide notice to individuals of the data they have collected and the purposes for that collection.

Also in contrast to the CCPA, the Virginia regime does not explicitly call for the creation of implementing regulations. While additional guidance will certainly be helpful to clarify how the VCDPA will be interpreted, businesses can and should begin planning their compliance strategies immediately, without questioning whether material provisions of the statute will change before the law goes into effect in 2023.

How the VCDPA Compares to the GDPR

The VCDPA borrows its core definitions—including its language about data “controllers” and “processors”—directly from the GDPR.¹⁹ Further, like the GDPR's requirement that data controllers consider “proportionality and necessity” when collecting personal information, the VCDPA also limits collection of personal data by controllers to that which is “adequate, relevant, and reasonably necessary in relation to

¹⁷ *Id.* at § 59.1-572(A).

¹⁸ *Id.* at § 59.1-571.

¹⁹ *Id.*

the purposes” of the processing of that data.²⁰ The VCDPA also aligns with common law standards for certain of its requirements, echoing the approach taken by the GDPR.

Novel to U.S. privacy laws, but similar to the GDPR, the VCDPA also imposes a requirement on data controllers to permit consumers to appeal any decision to deny a rights request.²¹ In addition to providing a right to appeal, the VCDPA also requires that, upon denial of an appeal, consumers must be informed about how to submit a complaint to the Virginia AG. As a result, companies may be more hesitant to reject consumer rights requests or complaints because of the possibility of follow-up action by the AG.

The most significant development under the VCDPA may be the institution of DPAs, which are similar to the DPIAs provided for under the GDPR, but are required in more settings under the Virginia regime, including whenever an entity covered by the VCDPA engages in specific types of activities. As a result, DPAs will be conducted more frequently than either the annual risk assessments required under the CCPA/CPRA or the DPIAs required under the GDPR. Additionally, unlike the annual risk assessments required by the CPRA, companies subject to the Virginia law are not required to voluntarily submit DPAs to regulators; they must, however, make the DPAs available at the request of the Virginia AG.²²

Implications:

- The VCDPA and CCPA/CPRA apply to businesses under different circumstances, making it important for businesses to assess anew whether they fall within the Virginia law.
- Data controllers may be incentivized by the VCDPA's exemptions to increase their use of de-identified or pseudonymous data in order to avoid the obligation to comply with consumer requests and minimize their potential liability under the statute.
- The use of DPAs as a mechanism of ensuring that specific types of activities are conducted in a manner that maintains the security of consumers' personal data is likely a development that will be incorporated into other states' data protection regimes, and one that imposes a potentially significant burden on entities seeking to comply.
- While companies with strong GDPR and CCPA compliance programs may enjoy a head start on ensuring compliance with the VCDPA, there are important differences between the statutory regimes that will require a specific focus on VCDPA compliance.

²⁰ *Id.* at § 59.1-574(A)(1).

²¹ *Id.* at § 59.1-573(B)(3).

²² *Id.* at § 59.1-575(A)(3).

-
- The passage of the VCDPA without reliance on a popular ballot initiative may indicate that there is momentum for other states with pending privacy legislation, such as New York, Washington, and Oklahoma, to pass their own data protection laws soon. That development, if it occurs, will further complicate the compliance obligations companies face and may increase pressure to pass a comprehensive federal data privacy law to supersede and simplify the laws in this space.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

Associates Julie L. Rooney and Cole A. Rabinowitz contributed to this Client Alert.