SULLIVAN & CROMWELL LLP

S&C memo

March 11, 2021

Virginia Consumer Data Protection Act

Virginia Is the Second State to Enact Comprehensive Privacy Legislation in the U.S.

SUMMARY

On March 2, 2021, Virginia enacted the Virginia Consumer Data Protection Act (the “VCDPA”), which will go into effect on January 1, 2023.

The VCDPA imposes a number of obligations on businesses that control or process personal data and grants consumers a range of new rights over their personal data. Consumer rights under the VCDPA include the right to: (1) receive notice of processing activity; (2) access personal data; (3) obtain a copy of the consumer’s data in a portable and readily usable format; (4) correct errors in personal data; (5) delete personal data; (6) opt out of behavioral advertising, automated profiling, and sales of personal information; and (7) avoid discrimination as a result of exercising consumer rights under the VCDPA. Importantly, the VCDPA does not create a private right of action for consumers.

The VCDPA applies to any entity that conducts business in Virginia or produces products or services that are targeted to Virginia residents, and that (1) annually controls or processes the personal data of at least 100,000 Virginia residents, or (2) controls or processes the personal data of at least 25,000 Virginia residents and derives over 50% of its gross revenue from the sale of personal data.[1]

The VCDPA borrows various concepts from the European Union’s General Data Privacy Regulation (“GDPR”), and provides for consumer rights similar to those provided by the California Consumer Privacy Act of 2018 (“CCPA”) and the recently enacted California Privacy Rights Act of 2020 (“CPRA”).

New York Washington, D.C. Los Angeles Palo Alto London Paris Frankfurt Brussels
Tokyo Hong Kong Beijing Melbourne Sydney

www.sullcrom.com

BACKGROUND

The VCDPA passed with overwhelming support in the Virginia General Assembly, including a unanimous vote in the Virginia Senate.[2] Governor Ralph Northam signed the legislation into law on March 2, 2021, making Virginia the second state (after California) to enact a comprehensive data privacy framework.[3]

A. KEY PROVISIONS

1. Categories of Rights

The VCDPA grants Virginia residents ("consumers") seven categories of rights:

- The Right to Know: Consumers have the right "to confirm whether a controller is processing the consumer's personal data."[4]
- The Right to Access: Consumers have the right to "access" personal data processed by a controller or processor."[5]
- The Right to Correct Inaccuracies: Consumers have the right to "correct inaccuracies in the consumer's personal data," based on the nature of the data and the purposes of the processing.[6]
- The Right to Deletion: Consumers have the right to "delete personal data provided by or obtained about the consumer."[7]
- The Right to a Copy: Consumers have the right to "obtain a copy of the consumer's personal data that the consumer previously provided to the controller" in a portable and readily usable (if technically feasible) format.[8]
- The Right to Opt Out: Consumers have the right to "opt out of the processing of personal data" for certain purposes, including (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling for decisions with legal or other significant effects on the consumer.[9]
- The Right to Avoid Discrimination: Controllers "shall not discriminate against a consumer for exercising any of the consumer rights" provided in the VCDPA.[10]

Controllers (described in more detail below) must provide consumers with a "reasonably accessible, clear, and meaningful privacy notice," which includes the type of and purpose for the personal data processed and whether third parties have access to that data.[11] If personal data has been sold to third parties or processed for the purpose of targeted advertising, the controller must "clearly and conspicuously disclose" that activity to the consumer.[12]

If a consumer contacts the controller to exercise any of its above-described rights under the VCDPA, the controller must respond within 45 days of receipt of the communication.[13] If a controller declines to act (as permitted in certain instances discussed below), it must notify the consumer within 45 days of receipt of the request, include a justification for the decision, and describe the process for appealing it.[14] The controller must provide a written explanation of its rationale for taking or declining to take action within 60 days of receiving an appeal.[15]

2. Controller vs. Processor Distinction

The VCDPA draws a distinction between controllers and processors of consumer data. A "controller" is a person or entity that "determines the purpose and means of processing personal data."[16] A "processor" is a person or entity that "processes personal data on behalf of a controller."[17] Processors include vendors such as email marketing companies, website hosting companies, and customer relationship management (CRM) companies. Processors are required to aid controllers to comply with the VCDPA, including by assisting controllers in fulfilling their obligation to respond to consumer rights requests, helping controllers meet their obligations to process personal data securely, and providing information to aid controllers to conduct and document data protection assessments under the VCDPA.[18]

Contracts between controllers and processors must include certain requirements, including that: (i) the processor is subject to a duty of confidentiality; (ii) the processor must, at the request of the controller, delete or return all personal data to the controller unless retention is required by law; (iii) the processor must, at the reasonable request of the controller, make all information in its possession available to the controller; (iv) the processor must allow and cooperate with reasonable assessments by the controller or a designated assessor; and (v) the processor may engage a subcontractor only if such subcontractor is also contractually required to meet the processor's obligations under the VCDPA.[19]

3. Personal Data and Sensitive Data

"Personal data" is defined in the VCDPA as "any information that is linked or reasonably linkable to an identified or identifiable natural person," excluding de-identified data or publicly available information.[20] The VCDPA also provides an opt-in right to the processing of "sensitive data," which includes all personal data relating to race, ethnicity, religion, health, sexual orientation, citizenship and immigration status, biometric data, personal data collected from a child, and precise geolocation data.[21] A consumer must consent to the processing of sensitive data, with "consent" defined as "a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer."[22]

4. Data Assessment Requirement

The VCDPA requires that controllers conduct data protection assessments for certain processing activities, including targeted advertising, profiling, sales of personal data, the use of sensitive data, and activities that "present a heightened risk of harm."[23] "Heightened risk of harm" is not defined, suggesting a potentially broad range of additional activities. The data protection assessments must weigh the benefits to the controller from the processing activities against the potential risks to the rights of the consumer as a result of such processing activities, factoring in the use of safeguards to mitigate those risks, the use of de-identified data (i.e. data that cannot be linked to an identifiable natural person), the reasonable expectations of consumers, and the relationship between the controller and consumer.[24] The office of the Virginia Attorney General ("AG") may request (through a civil investigative demand) that a controller disclose any data protection assessment relevant to an AG investigation under the VCDPA and may evaluate the assessment for compliance.[25]

5. De-Identified Data

Controllers in possession of de-identified data must take measures to ensure that it cannot be re-identified, publicly commit to maintaining and using such data without attempting to re-identify it, and contractually require any recipients of de-identified data to comply with these requirements.[26] Controllers are not required to comply with consumer requests under the VCDPA if the data is de-identified and (a) it would be unreasonably burdensome to associate the request with the personal data, (b) the controller does not use the data to recognize the consumer, and (c) the controller does not sell or disclose the personal data to any third party other than a processor.[27]

6. Public Enforcement / No Private Right of Action

The AG has exclusive authority to enforce the VCDPA.[28] If a controller or processor violates the VCDPA and does not cure such violation within 30 days of notice by the AG, the AG may seek an injunction and civil penalties of up to $7,500 per violation,[29] plus the reimbursement of the AG's reasonable expenses (including attorney's fees).[30] The VCDPA gives controllers and processors a 30-day cure period for all violations.[31]

The VCDPA also creates a special fund called the Consumer Privacy Fund, into which all civil penalties, expenses, and attorney's fees collected under the law will be paid.[32] Amounts paid into the Consumer Privacy Fund will be used to support the AG's enforcement of the law.

B. EXCEPTIONS & EXEMPTIONS

The VCDPA exempts certain categories of entities from its purview, including political bodies and agencies of the state, financial institutions subject to the Gramm-Leach-Bliley Act ("GLBA"), entities regulated by the Health Insurance Portability and Accountability Act ("HIPAA"), and institutions of higher education.[33]

The VCDPA provides for certain exceptions to data collection limitations imposed by the VCDPA where collection of such data is required to comply with law, to defend legal claims, to act at a consumer's request or for a consumer's safety or security, to conduct research in the public interest or internal research to improve products and services, or to perform internal operations that can be reasonably anticipated by the consumer.

The VCDPA also carves out certain categories of data from its limitations, including categories of information regulated by HIPAA, health records, patient identifying information, information relating to human research subjects, credit information, personal data covered by particular federal laws, and data collected about a controller's employees or independent contractors that is used in relation to such employees' and independent contractors' respective roles.

Finally, the VCDPA limits secondary liability. If a controller or processor discloses personal data to a third-party controller or processor and is in compliance with the VCDPA, it will not be found to have violated the law if the third-party recipient violates the law, so long as the disclosing party did not have actual knowledge that the recipient intended to commit a violation.[34] Similarly, a recipient controller or processor will not be found to have violated the law if the disclosing controller or processor violates the law.

C. IMPLICATIONS

The enacting of the VCDPA suggests the continuing shift in the U.S. toward more robust consumer data privacy. The VCDPA shows that state privacy regimes are starting to gain traction beyond California, a trend that is expanding the rights of consumers over their personal data and potential liability for businesses that collect personal data. Many other states are considering data privacy legislation, and two states—Oklahoma[35] and Washington[36]—have had consumer data privacy bills pass in one branch of the state legislature. The data privacy bills in New York and Florida have received wide public support, including from the governors of those states.[37] This movement in various states potentially adds pressure for Congress to consider national data privacy legislation in order to avoid a patchwork of state regulations that will complicate compliance for any company with multi-state operations.[38] Although there has not been any federal data privacy legislation proposed in 2021, several bills from 2020 have the potential to carry over into the new congressional term.[39]

Businesses that have taken steps to become CCPA and/or CPRA compliant should already be familiar with the steps that will be required to become VCDPA compliant. A business that is subject to the VCDPA should evaluate, and where appropriate update, its data collection and privacy policies and practices in at least the following respects:

1. Develop a comprehensive understanding of:

- the types of data it shares with third parties;
- the types of sensitive personal information it collects and how such sensitive personal information is used by the business; and
- the personal information it collects that is unnecessary for its disclosed purposes.

2. Prepare for the required disclosure of:

- the categories of personal information it processes;
- its purposes for processing personal data;
- how consumers may exercise their consumer rights under the VCDPA;
- the categories of personal data it shares with third parties, if any; and
- the categories of third parties, if any, with whom it shares personal data.

3. **Review its policies, procedures and systems required to:**

    - allow consumers to opt out of the use of their personal information for purposes prohibited by the VCDPA; and
    - provide the consumer with all personal information the business has collected about such consumer.

4. **Implement infrastructure to ensure its ability to respond to a request to correct.**

5. **Review and if appropriate amend contracts with service providers to include:**

    - an obligation for the service provider to comply with requests to delete personal information received from the business; and
    - an obligation to bind sub-processors to VCDPA obligations.

Businesses should also consider additional requirements that appear to be particular to the VCDPA, including by considering, where appropriate, the following measures:

- notifying consumers how a consumer may appeal a business's decision with regard to the consumer's request;
- identifying sensitive data and creating a consumer opt-in structure to comply with the VCDPA's requirements for the processing of sensitive data; and
- providing opt-out rights for the use of personal data for targeted advertising and profiling of Virginia consumers where such profile may have significant effects on the consumer.

*   *   *

ENDNOTES

[1] VCDPA § 59.1-572(A).

[2] *See Virginia Passes Consumer Privacy Law; Other States May Follow*, NAT'L L. REV. (Feb. 17, 2021), https://www.natlawreview.com/article/virginia-passes-consumer-privacy-law-other-states-may-follow.

[3] Rebecca Klar, *Virginia Governor Signs Comprehensive Data Privacy Law*, HILL (Mar. 2, 2021), https://thehill.com/policy/technology/541290-virginia-governor-signs-comprehensive-data-privacy-law.

[4] VCDPA § 59.1-573(A)(1).

[5] *Id.*

[6] *Id.* § 59.1-573(A)(2).

[7] *Id.* § 59.1-573(A)(3).

[8] *Id.* § 59.1-573(A)(4).

[9] *Id.* § 59.1-573(A)(5). The VCDPA defines a "sale of personal data" as any exchange of personal data for "monetary consideration." *Id.* § 59.1-571.

[10] *Id.* § 59.1-574(A)(4).

[11] *Id.* § 59.1-574(C).

[12] *Id.* § 59.1-574(D).

[13] *Id.* § 59.1-573(B)(1).

[14] *Id*. § 59.1-573(B)(2).

[15] *Id*. § 59.1-573(C).

[16] *Id.* § 59-1-571.

[17] *Id*. The VCDPA's definitions of "controller" and "processor" mirror the same terms used in the GDPR. *See* GDPR, Art. 4(7) ("'[C]ontroller' means the natural or legal person . . . which, alone or jointly with others, determines the purposes and means of the processing of personal data."); *id.* Art. 4(8) ("'[P]rocessor' means a natural or legal person . . . which processes personal data on behalf of the controller."). The CCPA and CPRA instead use the conceptually similar terms "business" and "service provider," which make a similar distinction between the entity that controls the processing of personal data (in the CCPA/CPRA, a "business") and the entity that processes information on behalf of another entity (in the CCPA/CPRA, a "service provider"). CPRA § 1798.140(d)(1) ("'Business' means: a . . . legal entity . . . that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information . . . ."). *Id.* § 1798.140(ag)(1) ("'Service provider' means a person that processes personal information on behalf of a business and which receives from or on behalf of the businesses a consumer's personal information for a business purpose pursuant to a written contract . . . .").

[18] VCDPA § 59.1-575(A).

[19] *Id.* § 59.1-575(B).

[20] *Id.* § 59.1-571.

[21] *Id.*

[22] *Id.*

[23] *Id.* § 59.1-576(A).

[24] *Id.* § 59.1-576(B).

ENDNOTES (CONTINUED)

[25] *Id.* § 59.1-576(C).

[26] *Id.* § 59.1-577(A).

[27] *Id.* § 59.1-577(C).

[28] *Id.* § 59.1-580(A).

[29] *Id.* § 59.1-580(C).

[30] *Id.* § 59.1-580(D).

[31] Under the CPRA, a similar 30-day cure period exists for private claims by consumers, but the newly established California Privacy Protection Agency may decide in its own discretion not to provide a time period to cure. CPRA §§ 1798.150(b), 1798.199.45.

[32] VCDPA § 59.1-581.

[33] This approach is distinct from the CCPA/CPRA, which only create exemptions for certain categories of data collected (e.g., nonpublic personal information collected by financial institutions subject to GLBA and protected health information subject to HIPAA).

[34] *Id.* § 59.1-578(D).

[35] http://www.oklegislature.gov/BillInfo.aspx?Bill=hb1602&Session=2000.

[36] https://app.leg.wa.gov/billsummary?BillNumber=5062&Initiative=false&Year=2021.

[37] Gary Detman & Jay O'Brien, *DeSantis Introduces Data Privacy Bill to Protect Floridians Personal Info*, CBS 12 (Feb. 15, 2021), https://cbs12.com/news/local/desantis-introduces-data-privacy-bill-to-protect-consumers-in-florida; *Governor Cuomo Announces Proposal to Safeguard Data Security Rights as Part of the 2021 State of the State* (Jan. 15, 2021), https://www.governor.ny.gov/news/governor-cuomo-announces-proposal-safeguard-data-security-rights-part-2021-state-state.

[38] *See* Rebecca Klar & Chris Mills Rodrigo, *New State Privacy Initiatives Turn Up Heat on Congress*, HILL (Feb. 10, 2021), https://thehill.com/policy/technology/538122-new-state-privacy-initiatives-turn-up-heat-on-congress.

[39] *See, e.g.*, S.2968, Consumer Online Privacy Rights Act, https://www.congress.gov/bill/116th-congress/senate-bill/2968; S.3300, Data Protection Act of 2020, https://www.congress.gov/bill/116th-congress/senate-bill/3300; S.3456, Consumer Data Privacy and Security Act of 2020, https://www.congress.gov/bill/116th-congress/senate-bill/3456/text.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.