GIBSON DUNN

Virginia Passes Comprehensive Privacy Law

Client Alert | March 8, 2021

On March 2, 2021, Governor Ralph Northam signed the Virginia Consumer Data Protection Act ("VCDPA") into law.[1] Virginia is only the second state to enact a comprehensive state privacy law, following California, yet its substance draws from both California's laws—the California Consumer Privacy Act ("CCPA"), and the newly enacted California Privacy Rights and Enforcement Act ("CPRA")—and a number of recently proposed state privacy bills. The Virginia legislature, however, is the first to enact such a law of its own accord – the California Legislature enacted the CCPA to preempt a ballot initiative in 2018 (and the CPRA was passed as a ballot initiative by California voters).

The VCDPA, which will go into effect on January 1, 2023, still differs from other enacted or proposed comprehensive state privacy laws in important respects, and companies doing business in Virginia or marketing to Virginians will need to reassess their collection and use of consumer personal information and modify their compliance efforts accordingly. The VCDPA will grant Virginia residents the rights to access, correct, delete, know, and opt-out of the sale and processing for targeted advertising purposes of their personal information, similar to the CCPA and CPRA. However, the VCDPA departs from its California counterparts and aligns with the European Union's General Data Protection Regulation ("GDPR") in a few key respects, including with respect to the adoption of data protection assessment requirements, and "controller" and "processor" terminology. The VCDPA also departs from the CCPA and CPRA by leaving enforcement entirely up to the Attorney General and not providing even a private right of action for consumers.

I. Background and Context

At the end of January and beginning of February, Virginia's House of Delegates and Senate overwhelmingly approved nearly identical versions of the VCDPA. Though Virginia was rarely mentioned among the states considering privacy legislation (such as Washington and New York) before 2021, state legislators managed to introduce and pass the VCDPA before the end of one of the country's shortest legislative sessions.[2]

Without the time to lengthily debate controversial issues that caused similar proposals in other states to die – such as the scope of a private right of action – the VCDPA focuses on privacy rights and obligations, over which there has been general consensus. Though the VCDPA does not call for the Attorney General to adopt regulations on how companies should implement it (whereas the CCPA and CPRA do), Senator David Marsden (D-Fairfax) told a Senate subcommittee that there would be sufficient time to "deal and field any tweaks to the bill or difficulties that someone figures out" before it takes effect on January 1, 2023.[3]

II. VCDPA's Key Rights and Provisions

A. Scope of Covered Businesses, Personal Data, and Exemptions

1. *Who Must Comply with the VCDPA?*

Related People

Ryan T. Bergsieker

Cassandra L. Gaedt-Sheckter

Frances Waldmann

VCDPA applies to all entities "who conduct business in the commonwealth of Virginia or produce products or services that are targeted to residents of the Commonwealth" and, during a calendar year, either:

> (1) control or process personal data of at least 100,000 Virginia residents, or
>
> (2) derive over 50% of gross revenue from the sale of personal data (though the statute is unclear as to whether the revenue threshold applies to Virginia residents only) and control or process personal data of at least 25,000 Virginia residents.[4]

In other words, the VCDPA will likely apply to for-profit and business-to-business companies that interact with Virginia residents, or process personal data of Virginia residents on a relatively larger scale. Just like the CCPA does not define "doing business" in California, the VCDPA does not define "conduct[ing] business in Virginia." However, businesses likely can assume that economic activity that similarly triggers tax liability or personal jurisdiction in Virginia will trigger VCDPA applicability.

Notably, unlike the CCPA, the statute does not include a standalone revenue threshold for determining applicability separate from the above thresholds regarding contacts with Virginia. Therefore, even large businesses will not be subject to VCDPA unless they fall within one of the two categories above, which focus on the number of Virginia residents affected by the business's processing of personal data.

The VCDPA contains a number of significant exclusions similar to, but broader than, those in the CCPA, with both entity-level and data-specific exemptions. For instance, the VCDPA exempts the following five types of *entities* (as opposed to just the *data* subject to certain laws): 1) Virginia state bodies and agencies; 2) financial institutions or data subject to the Gramm-Leach-Bliley Act ("GLBA"); 3) covered entities or business associates under the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act; 4) non-profit organizations; and 5) institutions of higher education.[5]

2. Definition of "Personal Data" – Employment and Public Data Excluded

As noted above, the Virginia law adopts GDPR terminology, referring to "personal data" (instead of "personal information," like the CCPA and CPRA), in addition to "controllers" and "processors." The statute defines "personal data" broadly to include "any information that is linked or reasonably linkable to an identified or identifiable natural person," but excludes employment data, pseudonymous data (a GDPR-borrowed term to mean personal data that cannot be attributed to an individual "without the use of additional information"), and "de-identified data or publicly available information."[6] Unlike the CCPA, the VCDPA extends the definition of "publicly available information" to information that has been "made available to the general public through widely distributed media," similar to the CPRA.[7]

B. Consumer Rights Mirror Those Granted Under the CPRA, But Go A Step Further

The term "consumer" includes Virginia residents and expressly excludes "any person acting in a commercial or employment context."[8] This represents a departure from the CCPA and GDPR and means that controlling or processing personal data in the business-to-business or employment context falls outside the scope of the law.

1. Access, correction, deletion, data portability, and anti-

discrimination rights

The VCDPA grants Virginia residents similar rights to those granted Californians under the CPRA, including the right to access, correct, and delete their personal information. Additionally, like the CCPA and CPRA, controllers must establish, as well as describe in their privacy notice, a secure means by which consumers can exercise such rights.[9] However, the VCDPA provides fewer exceptions than the CCPA/CPRA that controllers can leverage to deny consumers' request to delete their personal information.[10]

Though controllers cannot be required to re-identify de-identified or pseudonymous data to authenticate consumer requests, controllers can request additional information from the consumer without requiring them to create an account for authentication purposes.[11] The VCDPA, additionally, grants consumers the right to data portability, like the CCPA/CPRA and the GDPR. The VCDPA also grants consumers the right to not be discriminated against for exercising any of the rights granted thereunder, but explicitly exempts loyalty programs from this prohibition, like the CPRA.[12]

2. *Right to opt-out of sale of personal data, targeting advertising, and profiling*

Like the CCPA, the VCDPA grants consumers the right to opt-out of the sale of personal information but limits the definition of "sale" to the exchange of personal data for "*monetary*" (as opposed to "valuable") consideration by the controller to a third party, and does *not* include transfers to affiliates and processors.[13] Though the CPRA provides Californians with the right to opt-out of the sharing of their personal information for the purpose of cross-context behavioral advertising, the VCDPA goes a step further and grants Virginians the right to opt-out of any *processing* of their personal data for targeted advertising. The VCDPA also provides Virginians with the right to opt-out of any processing of personal data for the purposes of profiling for decisions that produce legal effects.[14] However, the VCDPA does not specify how controllers must present consumers with these rights to opt-out – thus, companies likely can leverage the "clear and conspicuous link" that it must provide to Californians on their homepages.

3. *New rights to opt-in to the processing of "sensitive" data and to appeal*

a) Right to opt-in to the processing of "sensitive" data"

The VCDPA requires that controllers obtain consent before processing a consumer's sensitive data,[15] defined as including "personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status"; genetic or biometric data processed for the purpose of uniquely identifying a natural person; the personal data collected from a known child; and precise geolocation data (as defined by the VCDPA).[16] Consent is 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" and may include "a written statement, including a statement written by electronic means, or any other unambiguous affirmative action."[17] The definition of "sensitive data" under the VCDPA is narrower than the equivalent "sensitive personal information" under the CPRA, although notably the processing of such data does not require express consent under the CPRA, and there is merely a right to *limit* processing of sensitive personal information (a limited opt-*out*).

Biometric data is defined as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual." This definition is reminiscent of the Illinois Biometric Information Privacy Act

("BIPA"), but potentially broader since the VCDPA does not limit its scope to specific types of biometric information. BIPA defines two regulated categories: biometric identifiers and biometric information. Biometric identifiers are "retina or iris scan[s], fingerprint[s], voiceprint[s], or scan[s] of hand or face geometry," and a number of items, such as written signatures and photographs are specifically excluded.[18] Biometric information under BIPA is defined to include any information based on an individual's biometric identifier that is used to identify an individual. The VCDPA also expressly excludes from the definition of biometric data physical or digital photographs, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.[19]

b) Right to appeal

Like the CCPA and CPRA, the VCDPA provides that controllers must respond to requests to exercise the consumer rights granted by the statute within 45 days, which period the controller may extend once for an additional 45-day period if it provides notice to the requesting consumer explaining the reason for the delay.[20] The VCDPA also grants consumers the right to appeal a controller's refusal of such a request through a novel "conspicuously available" appeal process to be established by the controller.[21] Within 60 days of receiving an appeal, a controller must inform the consumer in writing of its response to the appeal, including a written explanation of the reasons for the decision. If the controller denies the appeal, it must also provide the consumer with an "online mechanism (if available) or other method" through which the consumer can submit a complaint to the Attorney General.[22]

C. Business Obligations – Some New, Some Old

1. *Data minimization and technical safeguards requirements*

Like the CCPA/CPRA, the VCDPA limits businesses' collection and use of personal data and requires the implementation of technical safeguards. The VCDPA explicitly limits the collection and processing by controllers of personal data to that which is reasonably necessary and compatible with the purposes previously disclosed to consumers.[23] Relatedly, controllers must obtain consent from consumers before processing personal data collected for another stated purpose.[24] Also, like the CPRA and the New York Stop Hacks and Improve Electronic Data Security ("SHIELD") Act, the VCDPA requires that businesses establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data," as appropriate to the volume and nature of the personal data at issue.[25]

2. *GDPR-like requirements – data protection assessments and data processing agreements*

The VCDPA requires controllers to conduct "data protection assessments," similar to the data protection impact assessments required under the GDPR, to evaluate the risks associated with processing activities that pose a heightened risk – such as those related to sensitive data and personal data for targeted advertising and profiling – and the sale of personal data.[26] Unlike the GDPR, however, the VCDPA does not specify the frequency with which these assessments must occur.

Like Article 28 of the GDPR, the VCDPA also requires that the controller-processor relationship be governed by a data processing agreement.[27] These agreements require certain confidentiality and retention provisions, among others, and must "clearly set forth 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."[28]

The VCDPA does not displace or amend businesses' existing obligations under Virginia law to report data breaches.[29]

D. Enforcement – No Private Right of Action

The statute grants the Attorney General exclusive authority to enforce its provisions, subject to a 30-day cure period for any alleged violations. The Attorney General may seek injunctive relief and damages for up to $7,500 for each violation, as well as "reasonable expenses incurred in investigating and preparing the case, including attorney fees."

Notably, the VCDPA does not grant consumers a private right of action, unlike the CCPA/CPRA which grants a limited private right of action for consumers whose nonencrypted and nonredacted personal information was subject to unauthorized access and exfiltration.

* * * *

As we continue to counsel our clients through CCPA, and now CPRA, compliance, we understand what a major undertaking it is and has been for many companies. Some of the privacy rights and related obligations in the CCPA and CPRA are also featured in the VCDPA – companies can thus leverage their CCPA/CPRA compliance efforts in complying with the VCDPA. However, the VCDPA does grant Virginia residents new rights to consent to processing of "sensitive data" and to appeal decisions by companies to deny consumer requests. It also imposes new GDPR-type obligations on controllers – namely, the requirement to conduct data protection assessments and implement data processing agreements.

In light of this sweeping new law, we will continue to monitor developments, and are available to discuss these issues as applied to your particular business.

---

[1] The Virginia House of Delegates adopted the VVCDPA, H.B. 2307, on January 29, and the Virginia Senate approved an identical companion bill, S.B. 1392, on February 5.

[2] The legislative session was originally scheduled to end on February 11, 2021, but Governor Northam ordered a special session that ran through March 1, 2021.

[3] Hyung Jun Lee, *Virginia Lawmakers Advance Consumer Data Protection Act* (Feb. 18, 2021), available at https://www.washingtonpost.com/local/virginia-lawmakers-advance-consumer-data-protection-act/2021/02/18/a0cb8dba-7250-11eb-8651-6d3091eac63f_story.html.

[4] S.B. 1392 § 59.1-572(A).

[5] S.B. 1392 § 59.1-572(B).

[6] S.B. 1392 § 59.1-571.

[7] Id. The CPDA also excludes 14 categories of datasets, including data subject to the GLBA, Fair Credit Reporting Act, Drivers Privacy Protection Act, Farm Credit Act, and Family Education Rights and Privacy Act.

[8] Id.

[9] S.B. 1392 § 59.1-574(E).

[10] S.B. 1392 § 59.1-578(B).

[11] Id.; S.B. 1392 § 59.1-573(B)(4).

[12] S.B. 1392 § 59.1-574(A)(4).

[13] S.B. 1392 § 59.1-571.

[14] S.B. 1392 § 59.1-573(A)(5).

[15] S.B. 1392 § 59.1-57(A)(5).

[16] S.B. 1392 § 59.1-571.

[17] Id.

[18] 740 ILCS 14/10.

[19] Id.

[20] S.B. 1392 § 59.1-573(B)(1).

[21] S.B. 1392 § 59.1-573(C).

[22] Id.

[23] S.B. 1392 § 59.1-574(A)(1)-(2).

[24] Id.

[25] S.B. 1392 § 59.1-574(A)(3).

[26] S.B. 1392 § 59.1-576(A).

[27] S.B. 1392 § 59.1-575(B).

[28] Id.

[29] S.B. 1392 § 59.1-575(A)(2); Va. Code Ann. § 18.2-186.6.

This alert was prepared by Alexander H. Southwell, Ryan T. Bergsieker, Cassandra L. Gaedt-Sheckter, Frances A. Waldmann, and Lisa V. Zivkovic.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any of the following members of the firm's Privacy, Cybersecurity and Data Innovation practice group:

United States
Alexander H. Southwell – Co-Chair, PCDI Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
S. Ashlie Beringer – Co-Chair, PCDI Practice, Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com)
Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen – Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)

Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon – Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com)
Deborah L. Stein – Los Angeles (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner – Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com)

Europe
Ahmed Baladi – Co-Chair, PCDI Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox – London (+44 (0) 20 7071 4250, jacox@gibsondunn.com)
Patrick Doris – London (+44 (0) 20 7071 4276, pdoris@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Bernard Grinspan – Paris (+33 (0)1 56 43 13 00, bgrinspan@gibsondunn.com)
Penny Madden – London (+44 (0) 20 7071 4226, pmadden@gibsondunn.com)
Michael Walther – Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Alejandro Guerrero – Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic – Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen – London (+44 (0) 20 7071 4203, swazen@gibsondunn.com)

Asia
Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)

Related Capabilities

Privacy, Cybersecurity, and Data Innovation