ALERT MEMORANDUM

# The "New" Dominion of Privacy Law: Virginia Becomes Second State to Pass Comprehensive Consumer Data Privacy Act

*April 14, 2021*

Last month, Governor Ralph Northam signed the Virginia Consumer Data Protection Act ("CDPA" or "the Act") into law, making Virginia the second state in the nation to enact comprehensive data privacy legislation. The Act resembles and adopts some terms from the California Consumer Privacy Act ("CCPA"), the California Privacy Rights Act of 2020 ("CPRA"), which amends and expands the CCPA, and the European Union's General Data Protection Regulation ("GDPR"); however, the Act contains a number of distinctive provisions, compliance with which will require covered entities to adjust their privacy policies and practices, even if they are already CCPA and GDPR compliant, rendering the existing patchwork of state and national privacy laws even more complex.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors.

NEW YORK

**Daniel Ilan**
+1 212 225 2415
dilan@cgsh.com

**Rahul Mukhi**
+1 212 225 2912
rmukhi@cgsh.com

**Megan Medeiros**
+1 212 225 2072
mmedeiros@cgsh.com

**Melissa Faragasso**
+1 212 225 2115
mfaragasso@cgsh.com

Below we summarize key elements of the Act and highlight key similarities and differences with the CCPA and GDPR.

## Who must comply?

Beginning January 1, 2023, the CDPA will apply to entities that conduct business in Virginia or produce products or services that target Virginia residents *and* either (i) control or process the personal data of at least 100,000 Virginia consumers during a calendar year, or (ii) control or process the personal data of at least 25,000 Virginia consumers and derive 50 percent of gross revenue from the sale of personal data.[1]

A "consumer" is defined as "a natural person who is a resident of the Commonwealth acting only in an individual or household context." The term excludes any natural person acting in a commercial (B2B) or employment context.

Like the CCPA, the CDPA exempts (i) Virginia governmental agencies, (ii) non-profit organizations, (iii) institutions of higher learning, (iv) entities subject to the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act and (v) financial institutions subject to Title V of the Gramm-Leach-Bliley Act.

## What "personal data" is protected?

"Personal data" is defined as "any information that is linked or reasonably linkable to an identified or identifiable natural person." This definition exempts (i) publically available information[2] and (ii) de-identified data[3].

The CDPA also addresses the category of "sensitive data", and specifically prohibits the collection of sensitive data[4] without consumer consent. In contrast, the CCPA does not distinguish such "sensitive data" from other personal data, an omission that the CPRA rectified by defining a separate category of "sensitive personal information,"[5] and requiring that covered entities, at or

---

[1] The full text of the Virginia Consumer Data Protection Act is available here.

[2] Defined as "information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience."

[3] Defined as defined as "data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person."

[4] Defined as "a category of personal data that includes:

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

[5] Defined as "(l) personal information that reveals:

(A) a consumer's social security, driver's license, state identification card, or passport number;

(B) a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;

(C) a consumer's precise geolocation;

(D) a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;

before the point of collection, inform consumers of the collection of sensitive personal information. The CPRA also provides consumers with the right to opt out of the sale or *use* of sensitive personal data for reasons other than the provision of goods and services and prohibits covered entities from using sensitive personal information to infer characteristics about a consumer without providing the consumer with a right to limit such usage.

**What obligations are placed on covered entities?**

Like the GDPR, the Act makes a distinction between data controllers and data processors. Under the Act, data controllers are natural or legal persons, alone or jointly with others that determine the purpose and means of processing data, while data processors are natural or legal entities process personal data on behalf of a controller.

While both data controllers and data processors must adhere to the provisions of the Act, it is data controllers who are primarily responsible for most of the new obligations under the Act. Most notably, data controllers must:

- Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer;

- Refrain from processing personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;

- Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices must be appropriate to the volume and nature of the personal data at issue;

- Refrain from processing personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers; and

- Refrain from processing sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.).

---

(E) the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication;

(F) a consumer's genetic data;

and (2)

(A) the processing of biometric information for the purpose of uniquely identifying a consumer;

(B) personal information collected and analyzed concerning a consumer's health; or

(C) personal information collected and analyzed concerning a consumer's sex life or sexual orientation."

In addition to the above requirements, the Act contains a few additional obligations:

*Data Protection Assessments.* Data controllers must conduct data protection assessments of each of the following processing activities when the controller:

- Processes personal data for targeted advertising;
- Sells personal data;
- Processes personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of
    a. unfair or deceptive treatment of, or unlawful disparate impact on, consumers,
    b. financial, physical, or reputational injury to consumers,
    c. a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person, or
    d. other substantial injury to consumers;
- Processes sensitive data; or
- Engages in processing that presents a heightened risk of harm to consumers.

Data protection assessments must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks.

While the CCPA does not currently require data protection assessments, under the CPRA amendments, businesses that process personal information that presents a significant risk to consumers' privacy or security must conduct risk assessments with respect to the processing of such personal information and submit the report to regulators. Notably, these requirements are similar to GDPR's data protection impact assessment obligations.

*Service Providers' Data Processing Agreements*. Further, in a nod to Article 28 of the GDPR,[6] the CDPA requires data controllers and processors enter into data processing agreements whereby the parties "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." The CDPA requires such data processing agreements to contain certain obligations on data processors, including with respect to confidentiality, deletion/return of data, provision of information necessary to demonstrate compliance with the CDPA and auditing.

[6] Which requires controllers to only appoint processors who can provide sufficient guarantees of compliance with the GDPR and further restricts the processors actions to the documented instructions of the controller.

*Processing De-Identified Data.* The Act includes multiple exemptions with respect to the processing of de-identified data (data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person). While data controllers in possession of de-identified data must take reasonable measures to ensure that the data cannot be re-identified, publicly commit to maintaining and using de-identified data without attempting to re-identify the data, and contractually require any recipients of the de-identified data to comply with the aforementioned obligations, data controllers are exempt from complying with consumer requests to exercise their rights described below 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. [7]

Like the GDPR, the CDPA acknowledges pseudonymous data[8] as a category between personal data and anonymized or de-identified data. The CDPA exempts pseudonymous data from the scope of its data privacy rights, which means that the consumer rights discussed below (including access, correction and deletion rights) do not apply to pseudonymous data in cases where the controller is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

*Required Disclosure*s. Finally, the Act imposes an obligation to provide consumers with "a reasonably accessible, clear, and meaningful privacy notice," which must include (1) the categories of personal data processed by the controller; (2) the purpose for processing personal data; (3) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request; (4) the categories of personal data that the controller shares with third parties, if any; and (5) the categories of third parties, if any, with whom the controller shares personal data. Further, where a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must include a clear and conspicuous disclosure of the sale of personal alongside a mechanism in which the consumer can opt out.

---

[7] The CCPA establishes a high bar for claiming data is de-identified or aggregated, defining de-identified data as "information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses de-identified information:

(1) Has implemented technical safeguards that prohibit re-identification of the consumer to whom the information may pertain.

(2) Has implemented business processes that specifically prohibit re-identification of the information.

(3) Has implemented business processes to prevent inadvertent release of de-identified information.

(4) Makes no attempt to re-identify the information,

and aggregate consumer information as "information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device."

[8] Defined as "personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person."

**What rights do Virginia Consumers have under the Act?**

Under the CDPA, Virginia "consumers" are provided the following rights:

- *Access Rights*. The right to confirm whether or not a controller is processing the consumer's personal data and to access such personal data;

- *Correction Rights*. The right to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;

- *Deletion Rights*. The right to have personal data provided by or obtained about the consumer deleted;

- *Data Portability Rights*. The right to obtain a copy of the consumer's personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance; and

- *Opt-out Rights*. The right to opt out of (i) the processing of the personal data for purposes of targeted advertising, (ii) the sale of personal data, and (iii) the processing of personal data for purposes of profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

    - Importantly, the CDPA differs from the CCPA with regard to the definition of the "sale of personal data." Unlike the CCPA, the Act considers a "sale" to cover only "the exchange of personal data *for monetary consideration* by the controller to a third party," as opposed to the language of the CCPA which covers both "monetary or *other valuable consideration*". In this way, the Act more closely aligns with the Nevada Privacy of Information Collected on the Internet from Consumers Act, SB-220, which also narrowly defines "sale" as "the exchange of covered information for *monetary consideration* by the operator to a person for the person to license or sell the covered information to additional persons." Notably, disclosures to the controller's affiliates, to entities that processes personal data on behalf of the controller, or to third parties for purposes of providing product or service requested by the consumer, as well as disclosures as part of a merger, acquisition or other transaction in which a third party assumes control of the controller's assets, are exempt from the CDPA's definition of "sale."

In comparison, the CCPA and CPRA provide applicable consumers with many of the same rights, though the CCPA does not include the right to correct or rectify any inaccuracies in the personal information an entity holds about them. The CPRA reverses course and provides a right of rectification providing the consumer "the right to request [that] a business that maintains inaccurate personal information about the consumer correct such inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information."

**What are the penalties for non-compliance?**

Unlike the CCPA, which provides Californians a limited private right of action in relation to data breaches, the CDPA does not contain a private right of action for individuals. Instead, Virginia's Attorney General maintains exclusive authority to enforce the Act. Upon notification of a potential violation, covered entities have 30 days to provide the attorney general with an "express written statement that the alleged violations have been cured and that no further violations shall occur." Failure to cure alleged violations within the 30 days after being notified thereof may subject the entity to an injunction and civil penalties of up to $7,500 for each alleged violation. Furthermore, the Attorney General may elect to recover the cost of reasonable expenses incurred in investigating and preparing the case, including attorney fees.

All civil penalties, expenses, and attorney fees collected pursuant the Act will be credited to the Consumer Privacy Fund, which will be used to support the Office of the Attorney General with enforcement of the Act.

**Looking to the Future**

The past few years have seen an uptick in states working to enact data privacy legislation, and this trend is not slowing down. Currently, all eyes are on Washington and New York which are both positioned to pass privacy legislation at some point this year.

On March 3, 2021, the Washington State Senate voted 48-1 to pass the latest version of the Washington Privacy Act. The proposal is now in the House, which is working to act before the state's legislative session adjourns at the end of April. As currently drafted, the proposal would give consumers the right to access, correct and delete personal data collected by businesses, as well as require companies to issue privacy notices and adopt reasonable security standards. Similarly to Virginia, the law limits enforcement to the state's Attorney General, and provides no private right of action for consumers.

In New York, currently over 50 privacy bills have been introduced, such as the Biometric Privacy Act[9] (Assembly Bill 27) which was introduced on January 6 of this year. Current proposals of privacy bills include consumer rights of data access, control and transparency; however, unlike Virginia and Washington, some proposals include a private right of action for New York consumers. Moreover, some of the proposals also include a novel requirement that businesses act as "data fiduciaries," which would bar businesses from using consumer personal data in a way that benefits them to the detriment of the consumers. Most recently, Governor Cuomo has proposed his own comprehensive data privacy law that proposes the establishment of a Consumer Data Privacy Bill of Rights. The proposal sets out to guarantee New Yorkers "the right to access, control, and erase the data collected from them; the right to nondiscrimination from providers for exercising these rights; and the right to equal access to services."[10]

[9] See Cleary Blog Post: https://www.clearycyberwatch.com/2021/01/new-york-lawmakers-introduce-biometric-privacy-bill-with-private-right-of-action/

[10] https://www.governor.ny.gov/news/governor-cuomo-announces-proposal-safeguard-data-security-rights-part-2021-state-state

Though other states have also introduced similar legislation at the state level, federal lawmakers have also joined the fray. On March 10, 2021, Rep. Suzan DelBene, D-Wash., proposed the Information Transparency and Personal Data Care Act,[11] which would require companies to disclose with whom and for what reason they share consumer data, as well as requiring "affirmative, express, and opt-in consent" from consumers before they share personal and other sensitive data in unexpected ways. The proposal also provides the FTC the authority to write rules and assess penalties for first time violations of the law.

While debates continue over the efficacy of a federal model, experts seem more optimistic that with Democratic control over both Chambers of Congress and the Presidency, a federal law is very likely on the horizon. Until then, the patchwork of privacy laws across the country will likely continue to grow, increasing the necessity for companies to stay abreast of new and changing obligations with respect to the collection of consumer personal data.

…

CLEARY GOTTLIEB

[11] https://delbene.house.gov/uploadedfiles/delbene_consumer_data_privacy_bill_fact_sheet.pdf; https://delbene.house.gov/news/documentsingle.aspx?DocumentID=2740