Crowell

CLIENT ALERT

Virginia Consumer Data Protection Act (S.B. 1392)

March 3, 2021

The Virginia Consumer Data Protection Act (CDPA) has become the next major U.S. state privacy law, after being signed into law by Virginia Governor Ralph Northam on Tuesday, March 2, 2021. The new law amends Title 59.1 of the Code of Virginia with a new chapter 52 (creating Code of Virginia sections 59.1-571 through 59.1-581).

Who is covered?

Per Section 59.1-572, the bill applies to "persons that conduct business in the Commonwealth or that produce products or services that are targeted to residents of the Commonwealth" who "control or process personal data of at least 100,000 consumers" or those who "control or process the data of at least 25,000 consumers" AND "derive at least 50% of their gross revenue from the sale of personal data."

As defined in Section 59.1-571 the bill, "[c]onsumers" are any "natural person who is a resident of the Commonwealth acting only in an individual or household context. [Consumer] does not include a natural person acting in a commercial or employment context."

Both covered entities and "consumers" are defined more narrowly than under other general data privacy laws such as the California Consumer Privacy Act (CCPA). For example, in contrast to the CCPA's application to any California business with more than $25 million in annual revenue, the CDPA does NOT apply on a blanket basis to any Virginia business above a specified revenue threshold. To be covered under the CDPA, a person must always process the data of a minimum number of Virginia residents "acting only in an individual or household context." Additionally, the exemption for individuals acting in "commercial" or "employment" contexts is a complete one, and does not have a "sunset" date where the exemption will expire like the California law.

Notably, the CDPA follows the model established under the EU General Data Protection Regulation and categorizes relevant businesses as "controllers" and "processors." "Controllers" are "the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data," while "processors" are "a natural or legal entity that processes personal data on behalf of a controller." Similar to the controller/processor relationship created by the GDPR and the business/service provider relationship created under the CCPA, a CDPA processor must be engaged by a controller via a written agreement that governs the processor's data processing and provides specific instructions for the processing of data, as well as the nature and purpose of the processing.

Consumer rights under the CDPA:

Section 59.1-573 of the CPDA establishes a set of consumer rights increasingly familiar in the privacy world. Consumers may, via authenticated request to a controller:

1. Confirm whether their personal data is being processed by a controller;
2. Correct inaccuracies in their data;
3. Delete personal data obtained from or about the consumer;
4. Obtain a copy of the data the consumer previously provided the controller in a portable and "readily usable" format; and
5. Opt-out of data collection if the data is collected "for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer."

Controllers must respond to received requests within 45 days and may extend that period by a further 45 days when "reasonably necessary." Controllers must provide data in response to a request free of charge up to twice per calendar year and are only obligated to respond to requests that can be authenticated "using commercially reasonable methods." Controllers may request that consumers provide additional information "reasonably necessary" for the authentication of a request. If a request will be denied, controllers must inform consumers of the reasons for the denial, establish a "process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time" and respond to any such appeal within 60 days.

Obligations for Controllers:

A number of general affirmative obligations are imposed on controllers under the CDPA. Controllers must:

1. Limit collection of personal data to what is "adequate, relevant, and reasonably necessary" related to the purposes of processing, which must be disclosed to the consumer;
2. Refrain from processing personal data for any other purpose than those disclosed, unless the consumer consents;
3. "Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data."
4. Not process personal data in violation of anti-discrimination laws, or discriminate against consumers for exercising any consumer rights under the CDPA.
5. Refrain from processing "sensitive" consumer data without a consumer's consent.
6. Provide consumers with a "reasonably accessible, clear, and meaningful privacy notice" that includes:
    a. The categories of personal data processed by the controller;
    b. The purposes for processing the personal data
    c. How a consumer may exercise their CDPA rights, and how they may appeal a controller's decision regarding a request;
    d. The categories of data the controller shares with third parties;
    e. The categories of third parties the controller shares data with.
7. Provide clear and conspicuous notice to consumers of any sale of personal data to third parties or processing for targeted advertising, and the manner for opting out of such activity.
8. Create and provide in the privacy notice "one or more secure and reliable means for consumers to submit a request to exercise their consumer rights" that must "take into account the ways in which consumers normally interact with the controller" and the need for "secure communication of such requests."

a. Similar to the CCPA, controller cannot require consumers to create a new account in order to exercise consumer rights, though use of an existing account may be mandated.

Analysis: CDPA v. CCPA

As only the second major U.S. state privacy law, it is natural to compare the CDPA to California's CCPA (as recently amended by the California Privacy Rights Act (CPRA)), which until now has effectively been the high-water mark for U.S. consumer privacy compliance obligations.

Scope:

While there are some similarities between CDPA the CCPA, there are also a number of key distinctions between them. The scope of the CDPA is much more limited than either the CCPA (or the EU's GDPR) due to the lack of a general revenue threshold like CCPA Section 1798.140(c), which requires compliance by any California business with annual revenue over $25 million Additionally, the CDPA expands exemptions relative to the CCPA significantly. Individuals acting in "employment" or "commercial" contexts are totally exempt from the bill, a significant difference from the CCPA's exemptions for personal data collected in those contexts, where businesses are still required to give notice of the data collected and the purposes for collection.

Opt-outs and Exemptions:

Similar to the CCPA, Section 59.1-573(A)(5) of the CDPA allows consumers to opt out of "processing personal data for the purposes of …. (ii) the sale of personal data." Additionally, consumers may opt out of the processing of personal data for the purposes of both "(i) targeted advertising" and "(iii) profiling in the furtherance of decisions that produce legal or similarly significant consequences to the consumer." The ability of consumers to opt-out of the use of personal data for targeting and profiling as well as the sale of personal data might initially appear to expand the opt-out right relative to the CCPA. However, the interplay with the new exemptions will likely result in a much smaller practical impact due to the exemption for "publicly available" data. Section 59.1-571 of the CDPA defines the term "publicly available" to include "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," and "personal data" is explicitly defined to "not include … publicly available information." This is a significant change from the CCPA, which only defined as "publicly available" "information that is lawfully made available from federal, state, or local government records." As a result, data gleaned from individuals' public social media, or indeed any other "widely distributed media," (or shared about an individual by another party on social media) will not be subject to the law – likely welcome news for many in the advertising and data aggregation markets, as well as social media platforms themselves. How the CDPA's ultimate enforcer, the Virginia Attorney General, interprets "widely distributed media" will be a key issue if this bill becomes law in its current form.

The CDPA also shares a number of sector-specific opt-outs with the CCPA, including exemptions for data qualifying as Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA), information covered by the Fair Credit Reporting Act (FCRA), and information governed by the Family Educational Rights and Privacy Act (FERPA).

Sensitive Data:

In a notable similarity to the CCPA (as amended by the CPRA) and to Article 9 of the GDPR, the CDPA defines "sensitive personal data" separately from personal information in general. "Sensitive data" means 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.

While this category is not perfectly synonymous with either the CCPA or the GDPR, many of the items included are the same – including data about racial or ethnic origin, religious beliefs, sexual orientation. Also notable are the inclusions of both genetic or biometric data for identification purposes and precise geolocation data. Under the CDPA, controllers are required to obtain consumers' consent in order to process any "sensitive data" – and consent must be "a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action." Critically for many businesses, this definition would not permit "implied consent" or "consent by continued use of a service" without an affirmative consumer choice. This provision will also bring Virginia into the growing number of U.S. jurisdictions that affirmatively regulate the use of biometric and/or genetic data for the purpose of identifying individuals.

Enforcement:

A critical difference between the CDPA and CCPA is the issue of a private right of action. The CCPA creates a duty for businesses to "implement and maintain reasonable security" for personal information collected about California residents with a corresponding civil cause of action should a Californian's data be exposed as a result of a business' failure to do so. The CDPA does not create any private right of action, and leaves enforcement solely in the hands of the Virginia Attorney General, who must first "provide a controller or processor 30 days' written notice" of any alleged current or past violation. The controller or processor may, within the 30 days' notice, provide the Attorney General an "express written statement that the alleged violations have been cured and that no further violations will occur" and if such a representation is made, no action will be brought against the controller or processor. The Attorney General may seek "damages for up to $7,500 for each violation" of any continued breach of an express written statement so provided. The inclusion of a cure period and the lack of a private right of action together significantly reduce the exposure of businesses that will be subject to the CDPA.

When does the law take effect?

The CDPA will become effective on January 1, 2023. Notably, the CDPA will go into effect on the same day that the California Privacy Rights Act's (CPRA) changes to the CCPA go into force.

Appendix: Key Definitions:

"Authenticate" means verifying through reasonable means that the consumer, entitled to exercise his consumer rights in § 59.1-573, is the same consumer exercising such consumer rights with respect to the personal data at issue.

"Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.

"Consumer" means a natural person who is a resident of the Commonwealth acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context.

"Controller" means the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data.

"Decisions that produce legal or similarly significant effects concerning a consumer" means a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.

"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include de-identified data or publicly available information.

"Processor" means a natural or legal entity that processes personal data on behalf of a controller.

"Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

"Publicly available information" means 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.

"Sale of personal data" means the exchange of personal data for monetary consideration by the controller to a third party. "Sale of personal data" does not include:

1. *The disclosure of personal data to a processor that processes the personal data on behalf of the controller;*
2. *The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;*
3. *The disclosure or transfer of personal data to an affiliate of the controller;*
4. *The disclosure of information that the consumer (i) intentionally made available to the general public via a channel of mass media and (ii) did not restrict to a specific audience; or*

"Sensitive data" means 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.*

"Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests. "Targeted advertising" does not include:

1. *Advertisements based on activities within a controller's own websites or online applications;*
2. *Advertisements based on the context of a consumer's current search query, visit to a website, or online application;*
3. *Advertisements directed to a consumer in response to the consumer's request for information or feedback; or*
4. *Processing personal data processed solely for measuring or reporting advertising performance, reach, or frequency.*

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Kate M. Growley, CIPP/G, CIPP/US
Partner – Washington, D.C.
Phone: +1.202.624.2698
Email: kgrowley@crowell.com

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1.202.624.2775
Email: jposton@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1.202.624.2615
Email: ewolff@crowell.com

Maida Oringher Lerner
Senior Counsel – Washington, D.C.
Phone: +1.202.624.2596
Email: mlerner@crowell.com