MAYER | BROWN

March 10, 2021

Legal Update

Virginia's New Data Privacy Law: Comparing to California and Preparing for Next Steps

Virginia has become the second state to enact a comprehensive consumer data privacy statute in the United States. Signed into law by Virginia Governor Ralph Northam on March 2, 2021, the Consumer Data Protection Act ("CDPA") will take effect on January 1, 2023. While the CDPA shares some key components with the California Consumer Privacy Act ("CCPA") and the upcoming California Privacy Rights Act ("CPRA"), the CDPA also differs in several ways. Notably, one key difference is that the CDPA adopts a nomenclature that is more aligned with the terminology used in the European Union's General Data Protection Regulation ("GDPR") than in the CCPA or the CPRA. And, like the CPRA, the CDPA also includes certain requirements not included in the CCPA that will be familiar to companies that are subject to the GDPR.

What Should Companies Start Thinking About?

The first step for any company is to determine whether the provisions of the CDPA are likely to apply to data that the company collects or processes. As detailed in the "Scope of the CDPA" section below, the statute sets out a test and thresholds for companies that do business in, or target, Virginia consumers. If a company is likely to be subject to the CDPA, one of the first steps is to mark the calendar for November 1, 2021, to review implementation recommendations that will be submitted by a statutory working group (see the "Implementation" section below).

For companies that are already subject to the CCPA (and/or GDPR), there will be similarities to and overlap with certain compliance elements, such as in the area of data subject rights. One key distinction, which is likely to be new to most companies, is the opt-in consent requirement for "sensitive data"; companies should plan to take an inventory of the data they hold that may be considered "sensitive" under the CDPA, as well as the context in which it was collected or processed. If a company cannot be assured that it will have a valid legal basis for processing that data on January 1, 2023, when the CDPA comes into effect, it should put on its roadmap an interaction or touchpoint with consumers to obtain opt-in consent where feasible.

For companies that have not yet had to comply with the CCPA or GDPR but will be subject to the CDPA, the time before January 2023 provides an opportunity to conduct a data mapping and review of the company's privacy/data governance programs. These efforts, as well as the attendant compliance programs that are implemented, are a worthwhile investment, particularly as many state legislatures are actively considering comprehensive privacy laws. It is a reasonable assumption that Virginia will not be the last state to enact such a law.

Scope of the CDPA

The CDPA applies to entities that conduct business in Virginia or target Virginia residents and that either (1) control or process personal data of at least 100,000 Virginia consumers during a calendar year or (2) control or process personal data of at least 25,000 Virginia consumers and derive over 50 percent of gross revenue from the sale of personal data. Unlike the CCPA, the CDPA does not have a minimum revenue threshold for the law to apply. Borrowing a term from the GDPR, the CDPA refers to covered entities as "controllers."[1]

Under the CDPA, "consumer" is defined as a natural person who is a Virginia resident acting only in an individual or household capacity. The definition explicitly exempts a natural person acting in a commercial or employment context. "Personal data" is broadly defined in the CDPA as any information linked or reasonably linkable to an identified or identifiable natural person, with exceptions for "de-identified data" and "publicly available information." The definition of "publicly available information" aligns more closely with the CPRA than with the CCPA, which excludes only government records data. The CDPA (like the CPRA) excludes data lawfully made available from governments records, as well as information the business reasonably believes is lawfully made available to the general public through "widely distributed media," by the consumer herself or by a person or entity to whom the consumer has disclosed the information, provided the consumer did not restrict the intended audience (e.g., a public social media profile).

The CDPA has additional exemptions for both certain types of data and certain types of entities. Entities exempt from the CDPA include financial institutions subject to the Gramm-Leach-Bliley Act ("GLBA"), covered entities or business associates governed by the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), non-profits and institutions of higher education. Exempted data include data subject to the GLBA, protected health information under HIPAA, personal information subject to the Fair Credit Reporting Act ("FCRA"), employee/applicant personal data to the extent the data is collected within the context of employment or recruitment and several other types of data. (See the chart below comparing the CDPA, CCPA and CPRA at a high level.)

EXEMPTION	VA CDPA	CA CCPA	CA CPRA
Financial institutions and data subject to GLBA	Both exempt	Institutions not exempt Data Exempt*	Institutions not exempt Data Exempt*
Covered entities/business associates and protected health data under HIPAA and HITECH	Both exempt	Limited entities exemption Data exempt*	Limited entities exemption Data exempt*
Personal information subject to FCRA	Exempt	Exempt	Exempt
Employee/applicant personal data within employment context	Exempt	Exempt from most obligations until 1/1/2023*	Exempt from most obligations until 1/1/2023*
Personal data within business (B2B) context	Exempt	Exempt until 1/1/2023*	Exempt until 1/1/2023*
Non-profits	Exempt	Exempt	Exempt
Institutions of higher education	Exempt	Exempt if non-profit	Exempt if non-profit

* Subject to private right of action

Data Subject Rights Under the CDPA

The CDPA provides various rights to consumers concerning the personal data processed by a controller. Specifically, consumers have the right to:

- **Have a controller confirm whether it is processing[2] a consumer's personal data**
- **Access the consumer's personal data and obtain a copy of certain personal data in a portable format**
- **Correct inaccurate personal data**
- **Delete personal data provided by or obtained about the consumer**
- **Opt out** – Consumers may opt out of the processing of their personal data for purposes of (1) targeted advertising, (2) the sale of personal data or (3) profiling that produces legal or similarly significant effects on the consumer.

Non-discrimination – Controllers may not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers and may not discriminate against consumers for exercising any of their rights under the CDPA.

Responding to consumer requests – Controllers must respond within 45 days of receipt of a consumer request, which may be extended for an additional 45 days when "reasonably necessary," provided the controller notifies the consumer of the extension within the initial 45-day period.

Consumer right to appeal – Controllers must establish a process for consumers to appeal the refusal to take action on a request and must respond within 60 days of receipt of an appeal.

DATA SUBJECT RIGHTS	VA CDPA	CA CCPA	CA CPRA
Access	Yes	Yes	Yes
Correct	Yes	No	Yes
Delete	Yes (data provided by or obtained about consumer)	Yes (data collected from consumer)	Yes (data collected from consumer)
Portability	Yes	Yes	Yes
Opt-out of Sale	Yes	Yes	Yes
Non-discrimination	Yes	Yes	Yes
Appeals process	Yes	No	No

Controller Obligations

Controllers have the following additional obligations under the CDPA:

- **Data minimization** – Limit collection of personal data to what is adequate, relevant and reasonably necessary for the disclosed purposes for processing.
- **Purpose limitation** – Not process personal data for purposes that are neither reasonably necessary for the processing nor compatible with the disclosed purposes for processing unless the controller obtains the consumer's consent.
- **Security requirements** – Establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data.
- **Consent to process sensitive data** – Obtain consent from consumers for the processing of their sensitive data. "Sensitive data" includes (1) personal data revealing racial or ethnic origin, religious

beliefs, mental or physical health diagnosis, sexual orientation or citizenship or immigration status; (2) genetic or biometric data for the purpose of uniquely identifying a natural person; (3) personal data collected from a known child; and (4) precise geolocation data.

- **Privacy notice** – Provide a clear, reasonably accessible and meaningful privacy notice to consumers that describes (1) the categories of personal data processed by the controller, (2) the purposes for processing personal data, (3) how consumers may exercise their rights, (4) the categories of personal data shared with third parties and (5) the categories of third parties with whom the controller shares personal data.
- **Sale of personal data** – Clearly disclose the sale of personal data to third parties or the processing of personal data for targeted advertising, as well as the method by which a consumer may exercise the right to opt out of such sale or processing.
- **Data protection assessments** – Conduct and document a data protection assessment concerning the following types of processing activities: (1) targeted advertising, (2) sale of personal data, (3) profiling that presents a reasonably foreseeable risk of substantial injury to consumers, (4) processing of sensitive data and (5) any processing activities involving personal data that present a heightened risk of harm to consumers.
- **De-identified data** – (1) Take reasonable measures to ensure that the data cannot be associated with a natural person, (2) not attempt to re-identify the data and (3) contractually obligate any recipients of the de-identified data to comply with the CDPA.

The following chart provides a high level comparison of the controller or business-related obligations under the CDPA, CCPA and CPRA. Although certain obligations under the CDPA can also be found under the CCPA and CPRA, it is important to note that the specific requirements under these obligations may differ. For example, the definition of "sale of personal data" under the CDPA is narrower than the corresponding definition under the CCPA.

CONTROLLER OBLIGATIONS	VA CDPA	CA CCPA	CA CPRA
Data minimization	Yes	No	Yes
Purpose limitation	Yes	Yes	Yes
Security requirements	Yes	No, but the private right of action applies to security breaches	Yes
Consent for sensitive data	Yes	No	No, consumers can limit use to what is reasonably necessary
Special requirements for children's data	Yes (sensitive data of children under 13 years of age)	Yes (sale of personal information of children under 16 years of age and under 13 years of age)	Yes (sale of personal information of children under 16 years of age and under 13 years of age)
Privacy notice	Yes	Yes	Yes
Disclose sale	Yes	Yes	Yes
Data protection assessment	Yes	No	Yes, risk assessments submitted to CA Privacy Protection Agency
Requirements for de-identified data	Yes	Yes	Yes

Processor Obligations

The CDPA also sets forth certain requirements for "processors,"[3] namely that a processor must follow the controller's instructions and assist the controller in meeting certain of its CDPA obligations.

The CDPA requires a binding contract between a controller and a processor governing the processor's data processing procedures in which the following obligations must be included. These obligations align more closely with the GDPR's contractual requirements for processors than with the CCPA's contractual requirements for service providers:

- Instructions for processing data, the purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties;
- Duty of confidentiality for each person processing personal data;
- Deletion or return of all personal data to the controller, at the controller's discretion, at the end of the provision of services unless retention is required by law;
- Making available to the controller upon request all information in the processor's possession necessary to demonstrate the processor's CDPA compliance;
- Cooperation with reasonable assessments by the controller or the controller's designated assessor or arrangement for a qualified and independent assessment; and
- Requiring via a written contract any subcontractor to meet the obligations of the processor with respect to the personal data.

Implementation

Unlike the CCPA and CPRA, the CDPA does not authorize or require rulemaking or implementing regulations. Instead, the CDPA establishes a "work group" to consider "issues related to [the act's] implementation" and to submit findings, best practices and implementation recommendations to the chairmen of the Senate Committee on General Laws and Technology and the House Communications, Technology and Innovation Committee on or before **November 1, 2021**. The working group will include the secretary of commerce and trade, the secretary of administration, the VA attorney general (AG), the chairman of the Senate Transportation Committee, representatives from businesses that control or process the personal data of at least 100,000 persons and consumer rights advocates.

Enforcement

Unlike under the CCPA and CPRA, which contain a limited private right of action for data breaches, there is no private right of action under the CDPA. The VA AG will have exclusive authority to enforce the CDPA, subject to a 30-day cure period. If the controller or processor fails to cure violations of the act, the AG may bring an action and seek an injunction to restrain any violations, with civil penalties of up to $7,500 for each violation.

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

Vivek K. Mohan
+1 650 331 2054
vmohan@mayerbrown.com

Philip R. Recht
+1 213 229 9512
precht@mayerbrown.com

Lei Shen
+1 312 701 8852
lshen@mayerbrown.com

Jeffrey P. Taft
+1 202 263 3293
jtaft@mayerbrown.com

Howard W. Waltzman
+1 202 263 3848
hwaltzman@mayerbrown.com

Evan M. Wooten
+1 213 621 9450
ewooten@mayerbrown.com

Joshua M. Cohen
+1 312 701 8198
jmcohen@mayerbrown.com

Annemarie S. Kong
+1 312 701 8304
askong@mayerbrown.com

Endnotes

[1] A "controller" is defined in the CDPA as a "natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data."

[2] "Process" or "processing" is defined in the CDPA as "any operation or set of operations performed, whether by manual or automated means, on personal data or sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion or modification of personal data."

[3] A "processor" is defined in the CDPA as "a natural or legal entity that processes personal data on behalf of a controller."