The Computer & Internet Lawyer

Volume 38 ▲ Number 6 ▲ June 2021

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

New Virginia Privacy Law Promises Big Impacts

By Michael R. Young and Dorian W. Simmons

Virginia became the second state after California to pass a comprehensive privacy law when the governor signed the Consumer Data Protection Act ("CDPA"),[1] which contains many elements found in the California Consumer Privacy Act ("California Privacy Law") and other proposed privacy frameworks, as well as a number of new requirements for businesses.

This article pinpoints critical steps companies should take to ensure compliance, explains how the Virginia law is different from the California Privacy Law[2] and the European Union's European Union's General Data Protection Regulation ("GDPR"),[3] discusses the scope of the Virginia law and how it will be enforced, and describes consumers' opt-out and other rights.

Background

Upon signature by Governor Ralph Northam, Virginia became the second state (following California) to enact a comprehensive general privacy law. The CDPA shares common features with the California Privacy Law and state privacy bills but also contains its own unique requirements.

As a result of these unique requirements, companies subject to the CDPA, which is poised to take effect on January 1, 2023, will need to take specific steps to ensure that their data processing complies.

Scope of Application

Businesses may need to evaluate the scope of their data processing activities to determine if they collect and use information about Virginia residents subject to the CDPA. The CDPA applies to businesses operating in Virginia (or producing products or services marketed to Virginia residents) that meet one of the following thresholds relating to data activities:

- "Control or process" personal data of 100,000 or more Virginia consumers in a calendar year.
- "Control or process" personal data of at least 25,000 Virginia consumers and derive more than 50 percent of gross revenue from the sale of personal data.

"Processing" personal data includes virtually any collection or use of personal data. It includes, for example,

Michael R. Young, counsel on Alston & Bird's Privacy, Cyber & Data Strategy Team, focuses his practice on data privacy advising and technology transactions. **Dorian W. Simmons** is a senior associate on the firm's Privacy, Cyber & Data Security team. Resident in the firm's office in Atlanta, the authors may be contacted at michael.young@alston.com and dorian.simmons@alston.com, respectively.

"collection, use, storage, disclosure, analysis, deletion, or modification" of personal data.

"Personal data" means "any information that is linked or reasonably linkable to an identified or identifiable natural person."

"Consumer" includes individuals residing in Virginia; however, the CDPA defines "consumer" to expressly exclude individuals who act "in a commercial or employment context." Business-to-business contacts should not count toward calculating the total number of consumers to determine whether the CDPA applies.

Even if an entity otherwise meets these thresholds, the CDPA does not apply to:

- Financial institutions subject to relevant provisions of the Gramm-Leach-Bliley Act governing consumer privacy and security.

- Health care entities or their suppliers (referred to as "business associates") governed by privacy, security, and breach notice rules of the Health Insurance Portability and Accountability Act ("HIPAA") and related laws and regulations.

The CDPA also excludes certain kinds of information such as data created or maintained under certain federal health, financial, patient safety, education, or credit reporting laws.

Enforcement

The CDPA would go fully into effect January 1, 2023 and would empower the Virginia attorney general with broad exclusive authority to enforce the law. The CDPA states that it shall not "be construed as providing the basis for . . . a private right of action for violations of [the CDPA] or under any other law." The ultimate legal impact is likely subject to future litigation. (Notably, a similar statement appeared in the California Privacy Law and has not prevented plaintiffs' attorneys from citing that law to support claims under various legal theories.)

The attorney general may conduct a civil investigation if there is reason to suspect a violation. If the attorney general alleges that a business has committed a violation, the attorney general must provide the business with 30 days to cure the violation and provide the attorney general with a written statement that the violation has been cured and that no further violations will occur. If the business fails to cure the violation, the attorney general may seek to compel compliance (with injunctions) or seek civil penalties of up to $7,500 per violation.

Following the California model, collected penalties, expenses, and attorneys' fees will be paid into a dedicated "Consumer Privacy Fund" used to support further enforcement work by the attorney general.

The CDPA does not explicitly grant the state attorney general rulemaking powers. However, where the law leaves room for interpretation (e.g., data security), the attorney general could seek to issue further guidance, which would form a critical part of interpreting compliance obligations under the law.

Consumer Rights

Like other comprehensive privacy laws (such as the California Privacy Law and the EU's GDPR), the CDPA provides consumers numerous rights to their personal data. Consumers may exercise these rights against businesses that act as a controller.

Similar to the GDPR, a business acts as a controller under the CDPA if it determines the "purpose and means of processing" the personal data.[4]

If the business has reasonably verified the requestor's identity, the business must be prepared to respond to the following consumer requests:

- *Confirmation of Data Processing*. The business must confirm to the consumer whether the business processes personal data about that consumer.

- *Access*. The business must provide the consumer with access to their personal data. The CDPA does not expressly define what "access" requires. However, consistent with the interpretation of the right of access under other privacy laws, businesses should likely be prepared, at a minimum, to provide requesting consumers with the ability to view any personal data the business maintains about that consumer.

- *Correction*. The business must correct inaccurate personal data about the requesting consumer, "taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data." Note that the right of correction is not part of California's currently effective California Privacy Law (although it will become effective on January 1, 2023 under the California Privacy Rights Act, which amended the California Privacy Law).

- *Deletion*. The business is required to delete personal data provided by or obtained about that consumer. This right of deletion appears broader than the same right under the California Privacy Law, which only requires businesses to delete a consumer's personal information that businesses have collected from that consumer.

- *Portability*. The business must provide the consumer their data previously provided to the business in a portable and "to the extent technically feasible, readily usable format" that enables data transfers to other data controllers.

- *Opt-out*. Virginia's CDPA provides a set of opt-out rights from targeted advertising, sale of data, and certain profiling that may result in legally significant effects (such as the decision whether to offer a loan to the consumer).

Businesses must respond within 45 days to consumer requests. However, businesses may extend this period for another 45 days if "reasonably necessary" and with appropriate notice to the consumer.

Like other privacy rights laws, the CDPA appears to permit businesses to restrict their response to consumer rights requests in some instances.

For example, the CDPA states that it shall not be construed to restrict a business's ability to comply with law or legal processes, investigate or defend legal claims, provide products or services specifically requested by the consumer, or protect against fraud or security incidents.

A business may (and generally should) also limit its response to a consumer request if the requesting consumer's identity cannot be reasonably verified. (Providing access to a consumer's personal data to an unauthorized party may violate the controller's duty to implement reasonable security practices to protect the confidentiality, integrity, and accessibility of personal data.) In appropriate circumstances, businesses may reasonably limit their response to consumer rights in light of these and other exceptions under the CDPA.

However, businesses may not discriminate against consumers by, e.g., restricting service offerings in retaliation for the consumers' exercise of their rights.

Opt-Out Rights

The CDPA provides consumers with three distinct opt-out rights:

- *Opt-out of "targeted advertising."* Targeted advertising is defined as advertisements "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." Like other laws (most notably the California Privacy Rights Act), this provision appears aimed at giving consumers the option to limit the use of their information by online advertising networks that may track activity across websites or applications.

  This right poses an interpretive problem for businesses that do not themselves operate an advertising network but do permit third-party advertising networks to collect information on their websites. Do such businesses need to offer an opt-out if they are not themselves the data controller of an advertising network that profiles consumers?

  In the absence of guidance from the attorney general, many such businesses may decide to offer (or link to) such an opt-out to avoid potential risks.

- *Opt-out of "sale of personal data."* A business engages in the sale of personal data if it exchanges personal data for money. The CDPA clarifies that "sale" does not include certain exchanges of personal data, including the provision of personal data to a service provider, transfers for the purpose of providing a product or service the consumer requested, or in connection with a merger or acquisition.

  Unlike the California Privacy Law, the express definition of "sale of personal data" does not include the exchange of personal information for non-monetary consideration.

- *Opt-out of profiling having legal or "significant effects."* Virginia appears to be the first U.S. state to offer consumers an opt-out right for any automated processing of personal data (or "profiling") "in furtherance of decisions that produce legal or similarly significant effects" on consumers, though this concept may be found elsewhere internationally, for example within the GDPR. (California's Privacy Rights Act permits the state privacy regulator to issue regulations regarding automated decision-making, but no such regulations have been issued.)

  Such "significant" decisions include decisions whether to provide financial services (including loans) or "housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities." Businesses will need to evaluate whether they engage in automated processing having effects in these areas in order to honor relevant consumer opt-outs.

Consumer Rights Appeal Process

Businesses must establish an appeals process to allow consumers to appeal a business's decision not to act on a consumer rights request and inform consumers

of this process. As written, the CDPA appears to leave businesses with broad discretion to establish their own appeals process. This means, however, that businesses will face a number of decisions in creating an appeals process, including:

- Who will decide appeals?
- How independent (or not) will the appellate process be from other business operations? Will third-party adjudicators be used?
- Will consumers be permitted to submit additional statements or evidence or have discussions to present their point of view?
- How will appeals be presented to decision-makers to ensure impartiality?

A business has 60 days from an appeal request to inform a consumer of the business's decision and provide an explanation in writing. If a business denies an appeal through its appeals process, then it must provide the consumer with contact information for the Virginia attorney general, who is vested with broad authority to enforce the CDPA and investigate violations.

Practically, this may mean that unresolved consumer rights requests may result in review and investigations by the attorney general. Businesses should ensure that their compliance processes (including appeals) meet the rigorous scrutiny that may arise from consumer complaints to the attorney general.

Notices

Appropriate consumer notice is critical to support a business's data processing activity under the CDPA. Like other comprehensive privacy laws and proposals, the CDPA reflects a principle of limited collection. This means that personal data may only be collected and used to the extent disclosed in a privacy notice. Businesses must ensure that their notices reflect all relevant data collection and use activities.

The CDPA requires businesses to provide comprehensive disclosures of their processing practices for consumer personal data, including:

- Data collection.
- Purposes for processing.
- The categories of personal data shared with third parties.
- The categories of third parties personal data is shared with.
- Information about how consumers may exercise their rights, including their right to appeal.

In addition, businesses must provide some form of heightened ("clear and conspicuous") disclosure about sales of personal data or processing of personal data for targeted advertising.

These notice obligations are similar to those reflected in other laws, such as California's currently effective California Privacy Law.

Unlike California's law, the CDPA does not expressly require businesses to display a privacy notice at or before the point of the collection of personal data, nor does it require businesses to provide a "do not sell my information" link. As a result, businesses subject to California law may find that their existing privacy notices support many of the disclosures required by Virginia, or could do so with some adjustments to presentation.

Unusually for data protection laws, the CDPA additionally requires businesses to provide a "public commitment" for the use of deidentified data (i.e., data or a device that cannot reasonably be linked to an individual). Businesses must publicly commit not to reidentify such data.

For most businesses in most contexts, the logical form for such public commitment will be within public privacy notices; thus, businesses should be prepared to make public commitments about deidentified data within the relevant privacy notice. Though not expressly stated in the law, these requirements may fairly imply that businesses must assess whether they maintain any stores of deidentified data so that they can provide such appropriate notice and meet other control requirements for deidentified data.

Businesses must also take reasonable steps to prevent the reassociation of deidentified information with individuals and to contract with recipients to do the same.

Specific Consent Required to Process Sensitive Data

The CDPA prohibits any processing of sensitive data by a data controller without the consumer's consent. Both "sensitive data" and "consent" are defined in the CDPA:

- "Sensitive data" includes 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 used to identify a natural person; personal data collected from an individual known to be a child under the age of 13; and precise geolocation information identifying a person's location within 1,750 feet.

- "Consent" requires a "clear affirmative act" and must be free, "specific, informed, and unambiguous." Implied or opt-out consent likely does not meet this standard. In some circumstances, separate notices might reasonably be required to ensure that the consent is appropriately informed.

Because of this requirement, businesses that process sensitive data as a controller may face a significant impact in having to secure appropriate consumer consent for such processing.

Data Security

The CDPA requires that data controllers establish and maintain "reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data."

These standards are not defined in detail and likely present significant room for interpretation by the Virginia attorney general in enforcement, including in response to data breaches.

Controller / Processor Relations

Following a pattern set forth in EU and California privacy laws, the CDPA requires that businesses (acting as a controller) and their service providers (acting as a data processor at the direction of the business) contract for data protection. Contracts must include terms addressing:

- Confidentiality.
- Deletion or return of personal data at the conclusion of processing.
- The provision of information, upon request, necessary to demonstrate compliance.
- Support for assessments of compliance with the CDPA.[5]
- Subcontractor engagement.

In general, the required contractual content imposes obligations on data processors. Practically, these requirements are likely to result in substantial negotiations between controllers and service providers. Both businesses and controllers are therefore well advised to update forms and agreements sooner rather than later. Businesses that wait until the January 1, 2023 effective date to consider compliance likely will not be able to ensure that contracts reflect the required content.

In addition, the CDPA defines numerous independent responsibilities for data processors (i.e., responsibilities that stand apart from any particular contract with a data controller). Data processors are expected to limit processing, adhere to instructions from the data controller, provide appropriate assistance in support of data subject requests, support the response to data breach incidents, and support data protection assessments.

Data Protection Assessments

The CDPA requires data controllers to conduct "data protection assessments" when the controller conducts certain processing, including:

- Targeted advertising.
- Sales.
- Processing presenting "reasonably foreseeable" risks of harm, risk, injury, or unfair or unlawful treatment of consumers.
- Processing of sensitive data.

Businesses operating in the EU are likely to be familiar with the concept of data protection impact assessments.[6]

Similarly, under the CDPA, a data protection assessment requires identifying and weighing the risks and benefits of the potential data processing (to the business, the consumer, and "other stakeholders"). The assessment must consider the consumer's reasonable expectations and the relationship between the business and the consumer.

Notes

1. *https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+HB2307S1+pdf.*
2. *https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.*
3. *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.*
4. Businesses that act only as service providers on behalf of other businesses may not qualify as a controller unless they use personal data for their own (rather than their customers') purposes.

5. The CDPA provides some support for processors' use of "an appropriate and accepted control standard or framework and assessment procedure" to support assessment.
6. Under Article 35 of the GDPR, controllers are required to conduct a data protection impact assessment when the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons so controllers can assess the "particular likelihood and severity of the high risk" of a processing activity. Recital 90 (Data Protection Impact Assessment), Regulation (EU) 2016/679 (General Data Protection Regulation).