Virginia Poised to Enact the Consumer Data Protection Act, the Nation’s Second Comprehensive Consumer Privacy Law

Kyle R. Dull, Kyle R. Fath, and Patrick Waldrop
Among the CDPA’s requirements are:

- Consumer rights to:
  - Access, correction, transportability and deletion of personal data.
  - Opt-out of sale, processing for targeted advertising and profiling.
  - Opt-in to processing of sensitive data.
- Appeal rights for rejected consumer requests.
- Parental rights for known collection of personal data from children known to be under 13 in the vein of the federal Children’s Online Privacy Protection Act (COPPA).
- Data protection assessments for various types of data processing activities.
- Data processor regulation.
- Data security requirements.

The CDPA has no private right of action and will be enforced by the Office of the Virginia Attorney General, which can seek civil penalties after a 30-day opportunity to cure. Below, we provide an in-depth breakdown of the key elements of the bill.

Virginia’s Consumer Data Protection Act

In the CDPA, Virginia has developed a privacy bill that blends common concepts from familiar privacy regimes such as the CCPA and the European General Data Protection Regulation (GDPR) in a streamlined way. While a CCPA or GDPR compliance program can serve as a foundation for implementing a company’s CDPA obligations, there are material differences between the three regimes that will require somewhat different treatment of Virginian consumers.

The bill grants Virginian “consumers” the rights of access, correction, deletion and portability along with the right to opt out of targeted advertising, sales of personal data and automated individual decision-making. The CDPA also places similar requirements on controllers and processors of personal data, mandating certain contractual commitments. Helpfully, the bill excludes both business-to-business (B2B) and human resources (HR) data (though, with some nuance, as discussed below). Among the more innovative provisions are a right to opt out of processing of personal data for targeted advertising and the requirement to allow consumers to appeal denials of their rights requests. The CDPA is subject to the sole enforcement of the attorney general of Virginia; there is no private right of action under the bill (not even for security breaches like in the CCPA).
Classes of Covered Entities/Parties: The CDPA addresses “controllers,” “processors,” “third parties” and “affiliates,” each defined as follows:

- “‘Controller’ means the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data.”
- “‘Processor’ means a natural or legal entity that processes personal data on behalf of a controller.”
- “‘Third party’ means a natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller.”
- “‘Affiliate’ means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity. For the purposes of this definition, ‘control’ or ‘controlled’ means (i) ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company; (ii) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or (iii) the power to exercise controlling influence over the management of a company.”

The definitions of controller, processor and third party are virtually identical to the corresponding GDPR definitions. The definition of affiliate, on the other hand, is lifted nearly word-for-word from subparagraph 2 of the CCPA’s definition of a business. Like the CCPA’s treatment of businesses, the CDPA does not apply to all of these parties, but only those that meet certain requirements and data processing thresholds, discussed below.

Perhaps what is most interesting with regard to the entities covered by the CDPA is what is missing. It is something of a trend for recent privacy legislation to include the concept of a “data broker.” See, e.g., California Assembly Bill 1202 (passed in 2019 and codified as CA Civil Code Section 1798.99.80), Vermont Data Broker Law (V.S.A. ch. 62, subch. 5) and the New York Privacy Act (not yet passed).

The CDPA does not address the concept of the data broker.

Jurisdictional Scope: The CDPA applies to “persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth” and that meet one of two processing thresholds. This approach diverges from the CCPA and makes all defined parties – not just the “controller” – under the CDPA subject to definitional and collection thresholds in order to be subject to the law. This creates an interesting ambiguity in at least one respect, as controllers appear to have an absolute obligation to enter into contracts with processors (discussed below) irrespective of the processor’s meeting of the thresholds. On the other hand, there are explicit obligations on the processor, outside of the CDPA’s controller-processor contractual obligations, that would seem to clearly not apply if the thresholds are not met.

Moreover, it may be difficult for some vendors to determine whether the processing thresholds apply. While in many industries (such as AdTech) vendors have ways of determining the location of individuals, there are certain types of vendors that have no visibility whatsoever as to the data they are processing on behalf of their customers, let alone the location of individuals that can be identified from the data. These ambiguities will play out on a daily basis in the sometimes painful process of negotiating data processing agreements, where vendors will insist they are not subject to the law. The processing thresholds are as follows:

- First, the CDPA catches those who, “during a calendar year, control or process personal data of at least 100,000 consumers.”
- Meeting the second threshold requires “control[ing] or process[ing] personal data of at least 25,000 consumers and deriv[ing] over 50 percent of gross revenue from the sale of personal data.”

See § 59.1-572(A). Notably, the second threshold does not have a calendar year limit like the first, though the
intent and effect of the distinction is not apparent. Notably, the definition of “sale” is much narrower than under the CCPA and requires an “exchange” of personal data for monetary consideration under the CDPA, making the threshold narrower than the processing/sale thresholds in the CCPA.

Exceptions: A number of significant exceptions, including many similar to those in the CCPA, serve to carve out many types of organizations and many types of data from the CDPA’s scope. Per Section 59.1-572(B), the CDPA does not apply to the Virginia government; financial institutions subject to the Gramm-Leach-Bliley Act (GLBA); Health Insurance Portability and Accountability Act- and Health Information Technology for Economic and Clinical Health Act-covered entities or business associates; nonprofits; or “institutions of higher education.” The CDPA would, however, seem to capture processors of government entities, nonprofits and institutions of higher education that meet the data processing thresholds.

In addition to a host of health-related information being exempt including protected health information under HIPAA, information derived from any CDPA-exempt healthcare information that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA is exempt, as is “information used only for public health activities and purposes as authorized by HIPAA.” It appears that the latter exemption would address certain information used in relation to the ongoing COVID-19 pandemic, and the former will provide some flexibility for some health-related advertising use cases.

Broadly speaking, Section 59.1-572(C) also exempts information subject to other existing privacy regimes including the GLBA, the Fair Credit Reporting Act, and the Family Educational Rights and Privacy Act.

HR data is subject to overlapping exemptions and exclusions. First, HR data generally is subject to an exemption that is narrower than the one provided currently in the CCPA. Namely, HR data is only exempt “to the extent that the data is collected and used in the context of” the individual’s role as an applicant, employee, agent or independent contractor. See § 59.1-572(C)(14). Furthermore, “consumer” is defined to exclude “a natural person acting in a commercial or employment context.” B2B communications data is technically not exempt from the CDPA, as it is for the next two years under CCPA, but natural persons “acting in a commercial or employment context” are excluded from the definition of consumers. Practically speaking, therefore, B2B data is exempt from the CDPA.

Information Covered: The CDPA applies to “personal data,” defined to include “any information that is linked or reasonably linkable to an identified or identifiable natural person.” (Unless otherwise noted, all definitions are found in Section 59.1-571.) “Identified or identifiable natural person” is defined in the statute as “a person who can be readily identified, directly or indirectly.”

The definition of personal data goes on to explicitly exclude “de-identified data or publicly available information,” but not pseudonymous information. All three of these are defined in the CDPA:

- “De-identified data’ means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person.” Section 59.1-577 includes obligations as to de-identified data that are in line with the Federal Trade Commission’s requirements and which also will be adopted by the CPRA.
- “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.” This is similar to the definition provided under the CPRA.
- “Pseudonymous data’ means 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.” Unlike the CCPA, which defines pseudonymous data but invokes it minimally, the CDPA includes several consequential provisions, including in relation to consumer rights, where pseudonymous data is implicated.

As discussed in part above, Section 59.1-572(C) details 14 additional categories of information exempt, not technically from the definition of personal data, but from the statute generally.
Who It Protects: As the title of the bill suggests, the CDPA protects the “consumer.” The bill defines a “consumer” to be “a natural person who is a resident of the Commonwealth acting only in an individual or household context.” The definition does not define “resident” or tie it to the definition under tax laws, as is the case in the CCPA. It also does not provide for identifying someone as a consumer based on a unique identifier or more broadly, as the CCPA provides (“however identified”). That said, using an Internet protocol address or other information to determine location and thus residency, as is the practice of many businesses under the CCPA, would seem to be implicitly necessary under the CDPA in order to address a controller’s obligations as to pseudonymous data. Crucially, the definition goes on to explicitly exclude “a natural person acting in a commercial or employment context.” The CDPA therefore provides both the coveted B2B and HR data exemptions, though the HR data exemption is subject to some ambiguity and nuance as discussed above.

Key Concepts:

Consumer Rights, Controller Obligations and Appeals

Consumer Rights
The CDPA includes many of the consumer privacy rights we have become accustomed to already. Specifically, it provides that consumers may invoke the rights of access, correction, deletion and copies/portability along with the right to opt out of targeted advertising, sales of personal data and “profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.” See § 59.1-573(A)(1)-(5). The deletion right applies to personal data “provided by or obtained about the consumer,” whereas the CCPA’s right is narrower and only applies to information collected “from the consumer.” The CDPA’s right of access applies to the consumer’s personal data that the controller is processing, while the right to copies/portability only applies to personal data “that the consumer previously provided to the controller” and “where the processing is done by automated means.”

The CDPA provides that “[t]he consumer rights contained in subdivisions A 1 through 4 of § 59.1-573 and § 59.1-574 shall not apply to pseudonymous data.” See § 59.1-577.D. This excludes controllers from including pseudonymous information in fulfilling its obligations under the rights of access, correction, deletion and copies/portability, but only “in cases where the controller is able to demonstrate 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.” Id. The rights to opt out of targeted advertising, sales of personal data and profiling, however, would all apply to pseudonymous data. It is not clear whether the “consumer rights contained in” all of Section 59.1-574 or only those in subdivisions A 1 through 4 of Section 59.1-574 would not apply to pseudonymous data. If the former, it would exclude the requirement to obtain opt-in consent for processing of pseudonymous data that constitutes sensitive data (as set forth in Section 59.1-574(A)(5)); if the latter, controllers would have to obtain opt-in consent to process sensitive pseudonymous data (more on the opt-in to sensitive data later).

There is no right for agents to make requests on behalf of a consumer. However, a parent or legal guardian has the right to exercise CDPA rights on behalf of their child (defined as a natural person younger than 13 years of age). Opt-out rights are discussed in depth in the next section.

Controller Obligations
Sections 59.1-573(B)-574(E) prescribe how controllers should process consumer rights requests. Unlike the CCPA, there are no explicit requirements for how a controller must accept requests. Instead, Section 59.1-574(E) requires that controllers establish “one or more secure and reliable” request methods, “taking into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to authenticate the identity of the consumer making the request.” Similar to timing under the CCPA, controllers have 45 days to “respond” to each request, and that period is extendable by an additional 45 days unless the controller “declines to take action regarding the consumer’s request.” See § 59.1-573(B)(1)-(2). If the controller denies the request, the controller must inform the
consumer within 45 days of receipt of the request that the request is being denied and provide its justification for the denial and instructions for how to appeal the denial.

In one of the CDPA’s significant twists, Section 59.1-573(C) requires that controllers “establish a process for a consumer to appeal the controller’s refusal to take action on a request,” something permitted but not required by the CCPA. The details of the appeal process are sparse, but controllers must allow appeals submitted “within a reasonable period of time after the consumer’s receipt of the [controller’s] decision” and must make the appeal process “conspicuously available and similar to the process for submitting requests.” Following receipt of an appeal, a controller has 60 days to “inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions.” If the controller ultimately denies the appeal, the controller is also required to “provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.”

Finally, controllers are not required to comply with requests unless they are “authenticated” per Section 59.1-573(B)(4). Unlike the significant detail provided in the CCPA’s regulations as to verification of consumer requests, authentication is not defined in the CDPA, nor is there a specific process for authenticating prescribed, but Sections 59.1-573(B)(4) and 59.1-574(E) provide some clues as to what is intended and allowable:

- Controllers need only make “commercially reasonable efforts” to authenticate. (Controllers are not required to comply with a request if it cannot be authenticated “using commercially reasonable efforts.”)
- Additional information can be requested. (Controllers “may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer’s request.”)
- Existing accounts can be used. (“Controllers shall not require a consumer to create a new account in order to exercise consumer rights pursuant to § 59.1-573 but may require a consumer to use an existing account.”)

The Right to Opt Out of Sales, Targeted Advertising and Profiling

As mentioned above, the CDPA provides consumers the right “to opt out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.”

The CDPA defines “targeted advertising” as “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.” The statute goes on to provide several helpful exceptions to targeted advertising that clarify and narrow its scope significantly. “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.”

In some ways this definition is similar to the definition of cross-context behavioral advertising in the recent ballot initiative amendment to the CCPA (the CPRA), related to its “Do Not Share” right and covers traditional interest-based advertising activities. However, upon closer look, the CDPA’s definition of targeted advertising is a very limited definition that will seemingly exclude many digital advertising activities and use cases by certain parties that do not involve “displaying advertisements.” Importantly, too, it excludes from the definition of targeted advertising certain routine advertising activities, such as measurement and frequency capping, that exceed permissible purposes of service provider processing under the CCPA (though the CPRA rulemaking leaves the door open for revisiting these issues). As a result, those important activities will be able to continue even after a consumer has opted out.
of targeted advertising under the CDPA. One question the CDPA does not clearly answer is when a company is the controller of personal data that it processes for targeted advertising. Under the CCPA and CPRA, there are differing views as to whether the website publisher is the party responsible for providing an opt-out that would prevent the personal information from being collected by the AdTech cookie operator, or whether that party is acting independently and has the sole notice and choice obligation in the first instance. The same question can be asked under the CDPA – is the publisher processing the personal data of users of its site by allowing the AdTech company’s cookie to be integrated with the site?

With these exceptions in place, it is clear that the right to opt out of targeted advertising is not an opt out of contextual advertising or advertising analytics. The exception for advertisements based on activities within a controller’s own websites or online applications could also allow for meaningful digital advertising, including some types of retargeting, even after the consumer opts out. The targeted advertising opt-out is narrowly tailored and perhaps a good compromise between the advertising industry and privacy advocates. Complying with this opt-out right may even be as simple as directing consumers to already established opt-out mechanisms for interest-based advertising developed by the digital advertising industry self-regulatory bodies – the Digital Advertising Alliance and the Network Advertising Initiative – an approach that would not fully address “do not share” under CCPA, at least as those programs are currently operated.

The second opt-out right allows consumers to opt out of the sale of their personal data. Unlike the CCPA’s broad and unintuitive definition of sale, the CDPA defines the “sale of personal data” to mean “the exchange of personal data for monetary consideration by the controller to a third party.” It is exactly what any layperson would assume is meant by a sale of personal data, but the CDPA offers additional, helpful guidance by including exceptions, as seen with the definition for targeted advertising. “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” (similar to the exception for disclosures to a service provider under the CCPA or a contractor under the CPRA).
2. “The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer” (somewhat similar to the “intentional interaction” exception to sale under the CCPA, but potentially too narrow to permit opt-in to targeted advertising).
3. “The disclosure or transfer of personal data to an affiliate of the controller.” This is very consequential for groups of affiliated entities that share data among one another, as how to classify entities and transfers of personal information among them under the CCPA is a vexing issue (due in large part to poor drafting in the CCPA).
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.” This seems inspired by the CPRA’s expansion of the CCPA’s “publicly available” exception to “personal information.”
5. “The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction in which the third party assumes control of all or part of the controller’s assets.” The CCPA has a similar exception.

Finally, the CDPA grants consumers the right to opt out of “profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.” “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.” The right to opt out of profiling is therefore quite similar to the GDPR’s right to opt out of automated individual decision-making – a right that was curiously missing from the CCPA but incorporated by the recently passed CPRA.

**Limited Collection and Processing**

Section 59.1-574(A) places a number of requirements on controllers. First, 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.” See § 59.1-574(A)(1). Similarly, unless expressly allowed under the statute, controllers are prohibited from “process[ing] 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.” See § 59.1-574(A)(2). These purpose limitation requirements emphasize the importance of transparent disclosure and data minimization and are in line with requirements under the GDPR and forthcoming CPRA.

**Reasonable Security Practices**

Next, controllers must “[e]stablish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data.” The CDPA does not provide additional guidance on reasonable security practices except to say that “such data security practices shall be appropriate to the volume and nature of the personal data at issue.” See § 59.1-574(A)(3). There is no private right of action for breaches of security attributable to inadequate protection measures under the CDPA, though the attorney general could certainly bring an enforcement action pursuant to his enforcement powers (discussed below).

**Non-Discrimination and Loyalty Programs**

Like the CCPA, the CDPA prohibits discriminating against consumers “for exercising any of the consumer rights contained in [the CDPA].” See § 59.1-574(4). In fact, much of the language in this provision is lifted directly from the CCPA. The stated examples of what could constitute discrimination include “denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer.” This is strikingly similar to the language found in CCPA Section 1798.125(a)(1).

The next segment of Section 59.1-574(4) begins with language pulled from the CCPA, but takes a sharp turn:

> Nothing in this subdivision shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised his right to opt out pursuant to § 59.1-573 or the offer is related to a consumer’s voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

Emphasis added. Unlike the CCPA, the CDPA explicitly allows controllers to offer different prices or service levels to consumers who participate in a loyalty program or otherwise allow the controller to sell their data or process their data for targeted advertising or profiling, and does not require the valuations and value comparisons the California Attorney General maintains are mandated by the current CCPA regulations.

**Consent for Processing Sensitive Data**

The last segment of Section 59.1-574 requires that controllers obtain the consumer’s consent to process sensitive data about that consumer. See § 59.1-574(5). The CPRA adds an opt-out right for California consumers to some, but not all, uses for sensitive personal information. “Sensitive data” is 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."

This is a narrower articulation of personal data than is set forth in the CPRA’s definition of sensitive personal information; however, whether this list is exhaustive is ambiguous (because of the use of “includes”). Organizations that process any of this data should already be paying heightened attention to how they process it, but requiring consumer consent may be a challenging burden for some. Also, as mentioned above, there is some ambiguity as to whether the consent requirement applies to pseudonymous data that constitutes sensitive data.

“‘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.” As you might notice, this definition incorporates consent concepts familiar to those of us accustomed to the GDPR, and it is similar to the new consent standard introduced by the CPRA (though, consent is required in different contexts under the CPRA). As such, GDPR consent guidance may be instructive on how to obtain statutorily sufficient consent.

Children
Section 59.1-573(A) provides that “a known child’s parent or legal guardian may invoke consumer rights on behalf of the child regarding processing personal data belonging to the known child.” The CDPA defines a child as “any natural person younger than 13 years of age,” but does not specifically define a known child. It may indicate that obligations and rights relating to a known child only apply if the controller and/or processor knows the consumer is a child.

Per Section 59.1-574(A)(5), a controller cannot process “sensitive data concerning a known child, without processing such data in accordance with [COPPA].” As mentioned in the preceding section, “sensitive data” is defined by the CDPA to include, among other things, “personal data collected from a known child,” so this consent requirement effectively applies to all personal data collected from a known child. Section 59.1-572(D) similarly defers to COPPA, providing that “controllers and processors that comply with the verifiable parental consent requirements of [COPPA] shall be deemed compliant with any obligation to obtain parental consent under this chapter.”

All this taken together means that a controller cannot process personal data that it knows is being collected from someone under age 13 without COPPA-style parental consent. COPPA compliance is traditionally rather burdensome, but it is unclear how many organizations will need to develop COPPA-compliant consent mechanisms in response to CDPA because many organizations that collect personal data of known children are likely already subject to COPPA or exempt from the CDPA (e.g., nonprofits).

Privacy Notices
Sections 59.1-574(C)-(E) provide requirements for privacy notices that are similar to what we have seen in other laws such as the CCPA and GDPR, but with less prescriptive granularity than CCPA. Per Section 59.1-574(C), notices must be “reasonably accessible, clear, and meaningful” and include:

1. “The categories of personal data processed by the controller” (but CDPA does not enumerate what the categories are);
2. “The purpose for processing personal data” (without enumerating specific purpose categories);
3. “How consumers may exercise their consumer rights pursuant to § 59.1-573, 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.”

Meanwhile, Section 59.1-574(D) requires that a controller disclose that it “sells personal data to third parties or processes personal data for targeted advertising” and how a consumer may opt out of processing for targeted advertising or the sale of their data if the controller sells personal data or processes the data for targeted advertising.
Finally, as discussed previously, Section 59.1-574(E) obligates controllers to “describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights.”

Notably absent is a requirement for privacy notices to describe the rights granted to consumers by the CDPA. In fact, depending on the extent to which interest-based advertising is addressed, a typical CCPA notice would likely meet all of the CDPA’s requirements with only very minor changes.

Processor Requirements

As referenced above, the CDPA defines a processor to be “a natural or legal entity that processes personal data on behalf of a controller.” Section 59.1-575(A) specifies that “a processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this chapter.” The statute specifies that processors must reasonably assist controllers with responses to consumer rights requests, security, obligations related to a data breach experienced by the processor, and by providing necessary information to enable the controller to conduct and document data protection assessments. See § 59.1-575(A) (1)-(3).

Controllers and processors must also have a contract in place that meets certain requirements outlined in Section 59.1-575(B), which are very similar to the GDPR’s Art. 28 processor requirements. The contract 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 …[and] include requirements that the processor shall:

1. Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;
2. At the controller’s direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;
3. Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor’s compliance with the obligations in this chapter;
4. Allow, and cooperate with, reasonable assessments by the controller or the controller’s designated assessor; alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor’s policies and technical and organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request; and
5. Engage any subcontractor pursuant to a written contract in accordance with subsection C that requires the subcontractor to meet the obligations of the processor with respect to the personal data.”

Ultimately, any contract that meets the GDPR’s processor requirements will likely meet the CDPA’s requirements, alleviating the compliance burden for any organizations that have already implemented GDPR-compliant data processing agreements.

One issue that has perplexed many organizations and that is the subject of much debate under the CCPA is to what extent a vendor may process personal information for its own benefit and still retain the status of a service provider. Because “making available” personal information to a third party constitutes a sale under the CCPA, it is important to contractually limit a vendor’s processing to those purposes allowable of a service provider in order to prevent any such transfer from being a sale. The CDPA does not appear to present the same issue with respect to vendor processing for a number of reasons. First, there is not a contractual nexus between the designation of a party as a processor under the CDPA like there is a service provider under the CCPA. A processor is simply a “natural or legal entity that processes personal data on behalf of a controller.” To the extent that the processor exceeds its allowable purposes of processing the controller’s instructions and certain internal purposes set forth in Section 59.1-578(B), doing so would likely not implicate CDPA “sale” because there would be no exchange of personal data for monetary consideration.

Though the above sale issue may not arise out of the CDPA’s limitations on processors, we can likely expect to
see vendors designating themselves as co- or joint controllers instead of vendors, as is often the practice under the GDPR (particularly in certain industries such as AdTech) based on the processing activities required of them (in addition to other factors).

### Data Protection Assessments

Unlike the CCPA, but like the CPRA, the CDPA incorporates the GDPR requirement for controllers to conduct data protection impact assessments. The CDPA drops the “impact” though, preferring to use the term data protection assessment. Section 59.1-576(A) provides that data protection assessments must be conducted by controllers for “each of the following processing activities involving personal data:

1. The processing of personal data for purposes of targeted advertising;
2. The sale of personal data;
3. The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) 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 (iv) other substantial injury to consumers;
4. The processing of sensitive data; and
5. Any processing activities involving personal data that present a heightened risk of harm to consumers.”

Section 59.1-576(B) describes what a data protection assessment must include. Helpfully cutting down the number of such assessments that a controller is required to undertake, Section 59.1-576(D) provides that “a single data protection assessment may address a comparable set of processing operations that include similar activities,” while Section 59.1-576(E) states that “data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may comply under this section if the assessments have a reasonably comparable scope and effect.” This latter provision surely has the GDPR’s data protection impact assessments in mind.

Finally, the CDPA states in Section 59.1-576(F) that the data protection assessment requirement is not “retroactive,” instead applying only to “processing activities created or generated after [the CDPA’s effective date of] January 1, 2023.” This means that no assessments are necessary for processing activities commencing before 2023.

### Enforcement Risk: The CDPA does not include any private right of action. In fact, Section 59.1-579(C) bluntly states that “[n]othing in this chapter shall be construed as providing the basis for, or be subject to, a private right of action to violations of this chapter or under any other law.” Instead, Section 59.1-579(A) of the bill provides that “the Attorney General shall have exclusive authority to enforce violations of this chapter.” However, the CDPA does not provide any funding to the Attorney General at the offset. Virginia’s Department of Planning and Budget estimates that enforcing the CDPA would cost over $330,000 per year just in personnel costs. The CDPA sets up a fund to which all civil penalties shall be paid, which fund is intended to be used to support the work of the Attorney General to enforce the law. As with the original CCPA (but, which will go away under the CPRA), the CDPA requires the Attorney General to provide a 30-day cure period. Per Section 59.1-579(B), the Attorney General must provide “written notice identifying the specific provisions of this chapter the Attorney General, on behalf of a consumer, alleges have been or are being violated.” At that point, the controller or processor has 30 days to cure the noticed violation and submit “an express written statement that the alleged violations have been cured and that no further violations shall occur” to the Attorney General. If the controller or processor does so, then “no action for statutory damages shall be initiated against the controller or processor.” If, on the other hand, the controller or processor fails to cure the violation or otherwise continues its violations, “the Attorney General may initiate an action and seek an injunction to restrain any violation of this chapter and civil penalties of up to $7,500 for each violation under this chapter.”

Section 59.1-580 provides more detail on the Attorney General’s investigative and enforcement authority, including its ability to “issue a civil investigative demand to any controller or processor believed to be engaged in, or about to engage in, any violation of this chapter,” obtain an injunction, and collect civil penalties and attorney fees.
Regulations and Rulemaking: On Feb. 15, 2021, the House offered a substitute to the Senate bill, which included a new provision establishing a “work group composed of the Secretary of Commerce and Trade, the Secretary of Administration, the Attorney General, the Chairman of the Senate Committee on Transportation, representatives of businesses who control or process personal data of at least 100,000 persons, and consumer rights advocates … to review the provisions of this act and issues related to its implementation” and submit “findings, best practices, and recommendations regarding the implementation of this act … no later than November 1, 2021.” In addition, Virginia’s Attorney General does have rulemaking authority per Virginia administrative law. There are gaps in the statute that the Attorney General could choose to fill in with regulations.

Effective Date: Except for the establishment of the “work group”, the remaining provisions of the CDPA become effective in full on Jan. 1, 2023. The only caveat is that, as discussed above, the CDPA specifically provides that data protection assessments are not necessary for any processing activities “created or generated” before Jan. 1, 2023.

Conclusion

As with other major privacy compliance programs, organizations should prepare to handle new consumer rights requests, update privacy notices and implement compliant agreements with vendors. We should know very soon whether the CDPA will be enacted, which means organizations will have nearly two years to prepare for it to take effect. Two years sounds like a lot of time, but organizations that have not undertaken major privacy compliance programs should start as soon as possible, while organizations with established GDPR and/or CCPA compliance programs should review their programs now for CDPA compliance so that there is no chance of last-minute scrambling come Jan. 1, 2023.

For additional articles covering state privacy legislation updates, the CCPA, the CPRA or the recent Schrems II decision, including our 2020 year-in-review article, visit BakerHostetler’s Data Counsel blog and our Consumer Privacy Resource Center.