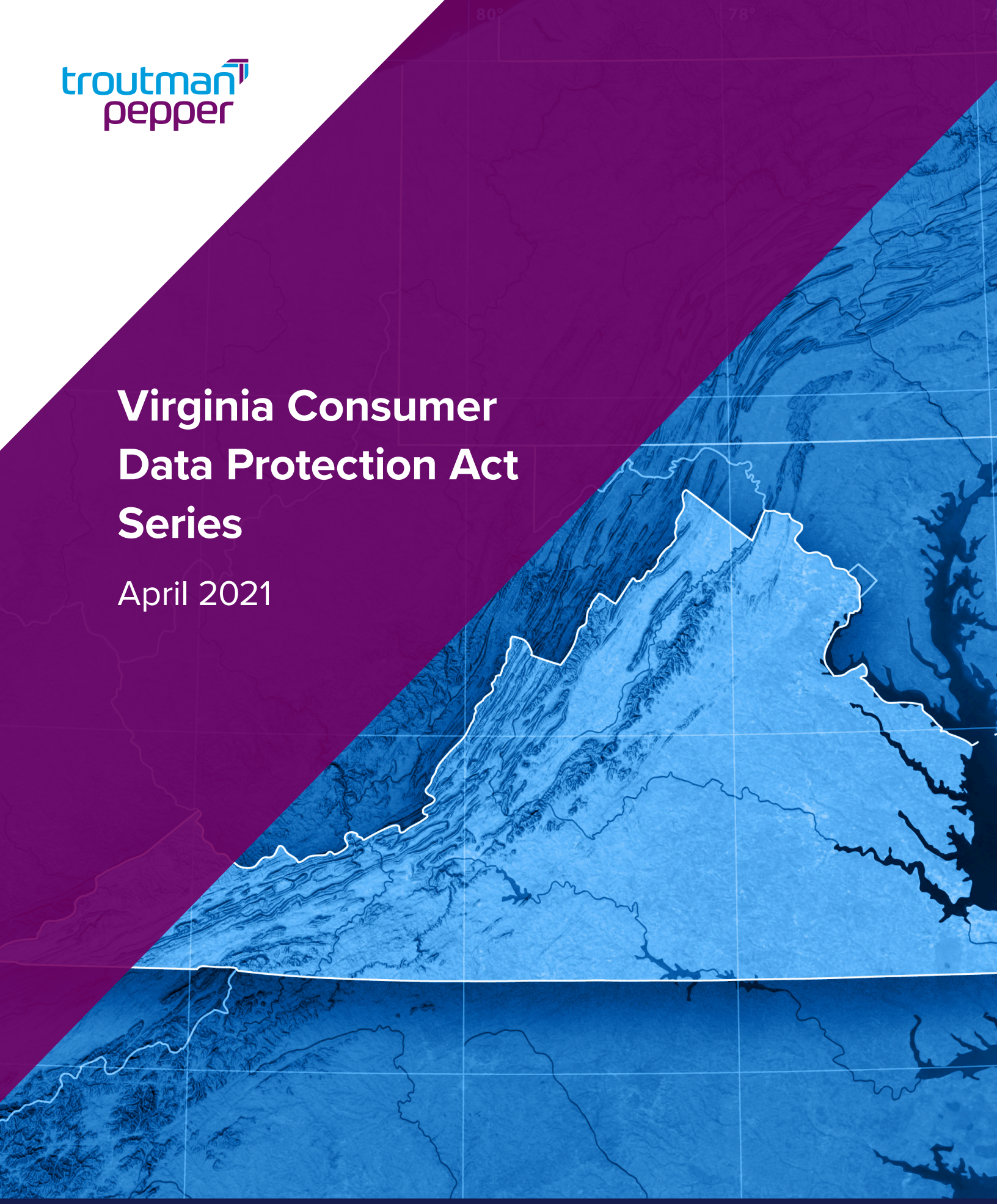
troutman pepper

Virginia Consumer Data Protection Act Series

April 2021



troutman.com

VCDPA Series: Part 1

Introduction and Overview

We have long predicted that just as other states followed California in passing breach notification laws, states would follow in California's footsteps in regulating information privacy practices with the California Consumer Privacy Act of 2018 (CCPA), which was later amended by the California Privacy Rights Act of 2020 (CPRA).[1] The Virginia state legislature recently became the first state to do so, surprising many with news that it quickly passed and signed into law comprehensive privacy legislation, namely the Virginia Consumer Data Protection Act (CDPA). Like the CCPA, Virginia's CDPA builds on the Fair Information Practice Principles (FIPPs), making many of the lessons learned implementing the CCPA applicable here. The CDPA will take effect January 1, 2023.

This five-part series on Virginia's CDPA provides a detailed overview of the act, and how it compares to California's approach to privacy under the CCPA and CPRA. The series will be divided into the following parts:

At the conclusion of the series, Troutman Pepper will host a webinar on the Virginia CDPA. Registration information will be circulated at a later date.

A. Why Virginia's CDPA is Similar to California's CCPA

It should come as no surprise that Virginia's CDPA is similar, but not identical to, California's CCPA. Indeed, as we discussed in our 2019 *Bloomberg Law* article, *So the CCPA is Ambiguous – Now What?*, all privacy laws derive from the same core foundational principals, namely the Fair Information Practice Principles (FIPPs). This includes, for example, the CCPA, CPRA, Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA), Health Insurance and Portability and Accountability Act of 1996 (HIPAA), Driver's Privacy Protection Act (DPPA), and even Europe's General Data Protection Regulation (GDPR).

Intended as guidelines that represent how organizations should collect and use personal information, the FIPPs recommend certain safeguards to ensure data collection practices are fair, and businesses are being transparent about their privacy practices. To this end, the FIPPs focus on adopting privacy frameworks that incorporate principles of *notice*, *choice*, *access*, and *security*. Because all privacy laws derive from these same core principles, it makes sense why we often see similar obligations and terminology across the different privacy laws. Notably, Virginia's CDPA borrows much of its terminology from Europe's GDPR (*e.g.*, the terms "controller" and "processor"), but also incorporates much of the text of the CCPA.

From a practical perspective, businesses seeking to comply with Virginia's CDPA should consider how these other privacy laws have been interpreted and enforced in the past.[2] By doing so, many of the challenges organizations may face with Virginia's CDPA — especially in the absence of implementing regulations — may become less obscure and enable organizations to make informed, well-reasoned compliance decisions still in line with their business goals.

[1] Unless stated otherwise, the term "CCPA" is intended to reference the CCPA and CPRA in general. Where we felt it was necessary to draw a distinction between the CCPA and CPRA, we did so by explicitly stating such.
[2] *See*, for example, Troutman Pepper's CCPA Enforcement Series, which identifies six areas of enforcement likely to catch the California office of the attorney general's attention.

B. Scope of Application: Who's Covered?

If your organization falls under the CCPA, then you know the CCPA primarily regulates "businesses." If you started your CCPA-compliance journey with Troutman Pepper, you may recall our infographic that breaks down the definition of a CCPA-regulated business, available here. In short, a CCPA-regulated "business" is any organization that (a) operates for the profit or financial benefit of its shareholders or other owners, (b) collects California consumers' personal information, (c) either alone or jointly with others, determines the purposes and means of the processing of consumers' personal information, and (d) meets certain threshold requirements.[3]

Entities that process personal information on behalf of regulated business are referred to as "service providers." While the obligations imposed on businesses by the CCPA are direct, a service provider's obligations under the CCPA are generally defined by the business in the applicable service provider contract.

For all practical purposes, a "business" under California's CCPA equates to a "controller" under Virginia's CDPA. Similarly, a "service provider" under California's CCPA corresponds to a "processor" under Virginia's CDPA. Those who deal with the GDPR will be familiar with these terms.

Entities are subject to the Virginia CDPA if they conduct business in the commonwealth or produce products or services that target residents of the commonwealth, and that:

- during a calendar year, *control* or *process* personal data of at least 100,000 consumers[4]; or
- *control* or *process* personal data of at least 25,000 consumers and derive over 50% percent of gross revenue from the sale of personal data.

Notably, Virginia's CDPA provides a "blanket exemption" from the act for (1) government agencies and authorities, (2) financial institutions subject to the GLBA, (3) "covered entities" or "business associates" regulated by HIPAA and HITECH, (4) nonprofit organizations, and (5) institutions of higher education. This differs slightly from California's approach, which provides an "information exemption" in certain contexts — meaning data regulated by certain laws, such as the GLBA and FCRA are exempt — but the entity itself may still be covered.

The below chart provides a comparison of the "blanket exemptions" under California's CCPA and CPRA and Virginia's CDPA.

Exemption	CA CCPA	CA CPRA	VA CDPA
Government Agencies	May depend on whether agency is "for-profit"	May depend on whether agency is "for-profit"	Exempt
Nonprofits	Exempt	Exempt	Exempt
GLBA-Regulated Financial Institutions	Not Exempt – but see Section C below	Not Exempt – but see Section C below	Exempt
Covered Entities and Business Associates Subject to HIPAA and HITECH	Not Exempt	Not Exempt	Exempt
Institutions of Higher Education	May depend on whether institution is "for-profit"	May depend on whether institution is "for-profit"	Exempt

[3] In order to qualify as a "business" under the CCPA, the business must also meet one or more of three thresholds: (1) the business has annual gross revenues in excess of $25 million dollars; (2) the business alone, or in combination, annually buys, receives for the businesses' commercial purposes, sells, or shares for commercial purposes, the personal information of 50,000 or more California consumers, households, or devices; or (3) derives 50% or more of its annual revenues from selling consumers' personal information. *See* Cal. Civ. Code § 1798.140(c). The CPRA slightly modifies threshold (2) by increasing the threshold from 50,000 to 100,000.

[4] "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 personal acting in a commercial or employment context.

C. Scope of Application: What Information is Regulated?

"Personal information" under California's CCPA equates to "personal data" under Virginia's CDPA. Both terms essentially mean any information linked or reasonably linkable to an identifiable person. Both California and Virginia exclude from the scope of their laws (1) information regulated by certain other privacy laws and (2) information that meets each state's definition of "de-identified" and "publicly available" information. Below find a high-level overview of the types of information that falls outside the scope of "personal information" under California's CCPA and CPRA and "personal data" under Virginia's CDPA.

Exemption	CA CCPA	CA CPRA	VA CDPA
Publicly Available Information	Exempt	Exempt	Exempt
De-Identified Data	Exempt	Exempt	Exempt
FCRA-Regulated Information	Exempt	Exempt	Exempt
DPPA-Regulated Information	Exempt	Exempt	Exempt
GLBA-Regulated Information	Exempt	Exempt	Exempt – *see* Section B above regarding "blanket exemptions"
HIPAA-Regulated Information, *i.e.*, PHI	Exempt	Exempt	Exempt – *see* Section B above regarding "blanket exemptions"
Information Collected in Employment Context	Exempt until January 1, 2023	Exempt until January 1, 2023	Exempt
Information Collected in Commercial/B2B Context	Exempt until January 1, 2023	Exempt until January 1, 2023	Exempt

Although not present in California's CCPA, both the California CPRA and Virginia CDPA introduce the concept of "sensitive" information/data and impose certain requirements relating to such. This follows Europe's GDPR approach, which provides specific protections when "special categories of personal data" are involved.

D. Consumer Rights

The second part of this series will cover the new consumer rights created by Virginia's CDPA, and how such rights differ in comparison to those offered under California's CCPA and CPRA. The below chart previews how the two states differ with respect to this issue.

Rights	CA CCPA	CA CPRA	VA CDPA
Access	✓ Yes	✓ Yes	✓ Yes
Delete	✓ Yes	✓ Yes	✓ Yes
Correct Inaccuracies	✗ No	✓ Yes	✓ Yes
Opt Out of Sale or Other Transfers	✓ Yes	✓ Yes	✓ Yes
Data Portability	✓ Yes	✓ Yes	✓ Yes
No Discrimination	✓ Yes	✓ Yes	✓ Yes

E. Notice and Disclosure Obligations

The third part of this series will cover the notice and disclosure obligations imposed by Virginia's CDPA, and how such obligations compare to those imposed by California's CCPA and CPRA. The below chart previews how the two states differ with respect to these issues.

Obligations	CA CCPA	CA CPRA	VA CDPA
Privacy Policy	✓ Yes	✓ Yes	✓ Yes
Notice at Collection	✓ Yes	✓ Yes	✗ No
Notice of Right to Opt Out	✓ Yes	✓ Yes	✗ No
Notice of Financial Incentive	✓ Yes	✓ Yes	✗ No

F. Data Processing Obligations

Service providers, and processors, and contractors, oh my! The fourth part of our series will detail the processing obligations imposed by Virginia's CDPA, and how such obligations compare to those under California's CCPA and CPRA. The article will focus on issues relating to data assessments and requirements relating to data minimization, obtaining affirmative consent to process certain types of information, and vendor contracts.[5] The below chart provides a high-level overview how the two states differ with respect to these issues.

Obligation	CA CCPA	CA CPRA	VA CDPA
Data Assessments	✗ No	✓ Yes	✓ Yes
Data Minimization Requirements	✗ No	✓ Yes	✓ Yes
Consent Requirements for Processing "Sensitive" Data	✗ No	✓ Yes	✓ Yes
Consent Requirements Relating to Children's Data	Yes, with respect to "sale" of personal information	Yes, with respect to "sale" of personal information	Yes, with respect to processing "sensitive data"
Vendor Contract Requirements	✓ Yes	✓ Yes	✓ Yes

[5] For organizations interested in learning more about the CCPA's obligations with respect to vendor contracts, see our Law360 article titled, "Calif. Privacy Law Means New Approach to Vendor Contracts."

G. Enforcement

We will put organizations out of their misery now and reveal that, like California's CCPA and CPRA, there is no private right of action for a violation of Virginia's CDPA. This was a contentious issue under the CCPA despite the statute's plain and unambiguous language, which provides that the California attorney general holds sole enforcement authority for CCPA violations but confers a private right of action in the data breach context.[6]

Part five our series will take a deep dive into the enforcement provisions of Virginia's CDPA, and how such provisions compare to those under California's CCPA and CPRA. For now, see our preview chart below on how Virginia's approach compares to California's.

	CA CCPA	CA CPRA	VA CDPA
AG Enforcement Authority for Act Violations of the Act	✓ Yes	Yes and the California Privacy Protection Agency	✓ Yes
Private Right of Action for Violations of the Act	✗ No	✗ No	✗ No
Requirements to Adopt Implementing Regulations	✓ Yes	✓ Yes	✗ No
30-Day Window to Cure Alleged Violations	✓ Yes	At the discretion of the California Privacy Protection Agency	✓ Yes
Statutory Damages	$2,500 - $7,500 per violation	$2,500 - $7,500 per violation	$7,500 per violation
Statutory Damages when Children's Data is Involved	$2,500 - $7,500 per violation	$7,500 per violation	$7,500 per violation
Private Right of Action for Data Breaches	✓ Yes	✓ Yes	✗ No

Contacts

Ron Raether
Partner
949.622.2722
ron.raether@
troutman.com

David Anthony
Partner
804.697.5410
david.anthony@
troutman.com

Ashley Taylor, Jr.
Partner
804.697.1286
ashley.taylor@
troutman.com

Edgar Vargas
Attorney
949.622.2473
edgar.vargas@
troutman.com

Sadia Mirza
Associate
949.622.2786
sadia.mirza@
troutman.com

Julie Hoffmeister
Associate
804.697.1448
julie.hoffmeister@
troutman.com

[6] A race to enforcement appears to be on the horizon. In Illinois, H.B. 3910 would grant the state attorney general enforcement powers, while H.B. 2404 would provide individuals with a private right of action. Massachusetts' S.B. 1726 would establish a state information privacy commission to handle enforcement. Minnesota's H.B. 1492 and Utah's S.B. 200 would empower the attorney general the right to take enforcement action against violators.

VCDPA Series: Part 2

Consumer Rights

As we noted in Part 1 of this series, which provides an introduction and overview of the Virginia Consumer Data Protection Act, most privacy laws — including those adopted in the United States — are built on the Fair Information Practice Principles (FIPPs). In part, the FIPPs establish a framework for allowing consumers to have more say over how their information is collected and used. To this end, the Individual Participation Principle states that an individual should have the right to access, correct, and delete their personal information.

Building on the Individual Participation Principle, the passage of the California Consumer Privacy Act of 2018 (CCPA) made California the first state to provide consumers with individual rights designed to give more control over the personal information that businesses collect about them. Less than two years later, the California Privacy Rights Act of 2020 (CPRA) amended the CCPA by, among other things, modifying the rights afforded to consumers. Most recently on March 2, Virginia became the first state to follow in California's footsteps with the passage of the Consumer Data Protection Act (CDPA). While similar to California in affording consumers certain rights over their personal information, the rights created by Virginia are different in several key respects. The below chart previews how the two states differ with respect to this issue, followed by a discussion on each right.

Rights	CA CCPA	CA CPRA	VA CDPA
Access	✓ Yes	✓ Yes	✓ Yes
Delete	✓ Yes	✓ Yes	✓ Yes
Correct Inaccuracies	✗ No	✓ Yes	✓ Yes
Opt Out of Sale or Other Transfers	✓ Yes	✓ Yes	✓ Yes
Data Portability	✓ Yes	✓ Yes	✓ Yes
No Discrimination	✓ Yes	✓ Yes	✓ Yes

Right to Access

The CCPA grants a consumer the right to obtain from a business[1]: (1) the categories of personal information it has collected about that consumer; (2) the categories of sources from which the personal information[2] is collected; (3) the business or commercial purpose for collecting or selling the personal information; (4) the categories of third parties with whom the business shares personal information; and (5) the specific pieces

[1] The CCPA and CDPA utilize the defined term "business" to refer to an entity that alone, or jointly with others, determines the purposes and means of processing of personal information. The CDPA refers to this entity as a "controller."

[2] The CCPA and CPRA use the term "personal information," which is defined as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." The CDPA uses the term "personal data," which is defined as "any information that is linked or reasonably linkable to an identified or identifiable natural person." We use the term "personal information" when discussing the CCPA and CPRA and the term "personal data" when discussing the CDPA.

of personal information collected about that consumer. The CCPA imposes a 12-month lookback from the time of the request.

The CPRA will extend that 12-month window indefinitely (beginning January 1, 2022)[3], requiring that businesses provide access to all categories of personal information collected "unless doing so proves impossible or would involve a disproportionate effort." Neither "impossible" nor "disproportionate effort" are defined by the CPRA.

Virginia's access right does not include disclosure of any categories of information or the business or commercial purposes for collecting or selling the personal information. Instead, Virginia consumers have the right to (1) confirm whether or not a controller is processing the consumer's personal data and (2) access such data (likely similar to the CCPA's requirement that businesses disclose "the specific pieces of personal information collected"). Unlike the CCPA, there is no lookback period limiting the data that must be disclosed.

Right to Delete

Under the CCPA, California residents have the right to request that a business delete any personal information about the consumer that the business collected from the consumer. Upon receipt of a request to delete, businesses must delete the consumer's personal information from its records (subject to certain exemption) and direct its service providers[4] to do the same.

Though leaving the basic CCPA framework the intact, the CPRA expands the consumer's "right to delete" in several key respects. In addition to directing service providers to delete consumer's personal information from their records upon receiving a verifiable consumer request, the CPRA also requires businesses to notify "contractors" to delete the personal information, "and notify all third parties to whom the business has sold or shared such personal information, to delete the consumer's personal information, unless this proves impossible or involves disproportionate effort." The CPRA does not, however, define what qualifies as "disproportionate effort." Finally, the CPRA places direct obligations on service providers and contractors that have been notified of a deletion request by the business to in turn notify any service providers, contractors, or third parties who may have accessed such personal information from or through the service provider or contractor.

The CDPA affords Virginia consumers a more expansive right to delete by mandating that, upon receipt of an authenticated consumer request, a controller delete personal data provided by or obtained about the consumer, rather than just data collected "from the consumer," as is the case with the CCPA. And while there is no express requirement that a controller instruct third parties with whom the consumer's personal data was sold or shared to delete that data, the CDPA does require that processors assist controllers in fulfilling the controller's obligation to respond to a consumer rights request, including a deletion request, "taking into account the nature of the processing and the information available to the processor, by appropriate technical and organizational measures, insofar as this is reasonably practicable." The phrase "reasonably practicable" is not defined.

Right to Correct Inaccuracies

The right to correct refers to the ability of a person to request that a business rectify any inaccuracies in the personal information that it holds about them. While the California Online Privacy Protection Act

[3] The CPRA only applies to personal information collected by a business on or after January 1, 2022. Otherwise, the provisions of the CCPA apply.

[4] The CCPA and CDPA refer to the entity that processes personal information on behalf of a business as a "service provider." The CDPA refers to that entity as a "processor."

(CalOPPA) encourages businesses to consider offering customers the opportunity to review and correct their personal information, the California legislature did not include this right within the CCPA. Unlike the CCPA, however, CPRA does contain a right to correct inaccurate information. Specifically, the CPRA provides consumers with the right to "request a business that maintains inaccurate personal information about the consumer to correct that inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information … ." Further, if such a request is received, a business is required to "use commercially reasonable efforts to correct the inaccurate information."

Similarly, Virginia's CDPA provides that a consumer has the right "[t]o correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data." The types of processing that may not warrant correcting consumers' personal data is not defined by the CDPA. One potential example, however, may be data used to detect security incidents or fraud. Another example could be where the business has a legal obligation to preserve the data, such as a lawsuit concerning data that a consumer requested to be corrected.

Right to Opt Out of Sale or Other Transfers

The CCPA gives consumers the right to direct a business not to sell their personal information to a third party. "Sell" is expansively defined in the CCPA as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party *for monetary or other valuable consideration*." The CCPA clarifies, however, that the following activities do not qualify as "sales": (i) disclosing data at the direction of the consumer; (ii) using an identifier to alert third parties that a consumer has opted out; (iii) sharing information with service providers, so long as the service provider does not use or sell the personal information for their own purposes; and (iv) disclosing personal information as an asset in a merger, acquisition, or similar transaction.

The CPRA expands the CCPA's opt-out right in several respects:

- to allow a consumer to opt out of the "sharing" of personal information, which is defined as the transfer or making available of a "consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration";
- to allow a consumer to limit the use and disclosure of "sensitive information" to that "which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods and services," subject to certain exemptions; and
- to request information about the logic behind a description of the likely outcome of and to opt out of the use of automated decision-making technology in connection with decisions about the consumer's work performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

By contrast, Virginia's CDPA gives consumers the right to "opt out of the processing of 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."

Importantly, a "sale" of personal data is more narrowly defined than it is in the CCPA or CPRA. Indeed, Virginia limited its definition of "sale" to "the exchange of personal data for *monetary consideration* by the controller to a third party," and therefore did not incorporate the controversial "other valuable consideration" language found in the CCPA. Critics of the CCPA often note that the phrase "other valuable consideration" is so broad that any exchange of personal information could arguably meet the

CCPA's definition of "selling." By not including this language in its own definition, Virginia has simplified what qualifies as "sale" to only those instances where personal data is exchanged for money.[5]

Virginia's CDPA also excludes from the definition of "sale" the disclosure of personal data: (i) to a processor; (ii) to an affiliate; (iii) that the consumer "intentionally made available to the general public via a channel of mass media" and "did not restrict to a specific audience"; or (iv) is disclosed as an asset in a merger, acquisition, or similar transaction.

Right to Data Portability

The CCPA gives consumers the right to obtain a copy of their personal information "in a readily useable format that allows the consumer to transmit [the] information from one entity to another entity without hindrance." In effect, this requirement gives consumers a data portability right, since they can migrate their personal information from one business to another offering similar services. This right was modified by the CPRA to require businesses to provide copies of the personal information obtained from the consumer "in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format, which also may be transmitted to another entity at the consumer's request without hindrance."

The CDPA provides a more limited right to data portability. *First*, the CDPA only requires that the controller provide a portable copy of the personal data "that the consumer previously provided to the controller," not all of the data that was collected concerning the consumer. *Second*, the requirement that, to the extent technically feasible, the data be provided in a readily useable format that allows the consumer to transmit the data to another controller without hindrance is limited by the provision that such format is only required "where the processing is carried out by automated means." The phrase "where the processing is carried out by automated means" is also not defined or further explained. The CDPA, however, defines processing as "any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage disclosure, analysis, deletion or modification of personal data." By adding the plain meaning of automated (not requiring human intervention), the phrase may limit a consumer's right to receive a portable and readily usable copy of the data solely to data that is processed without human intervention.

Right to be Free from Discrimination

The CCPA prohibits businesses from "discriminating" against consumers who exercise the rights granted to them by the CCPA but does not define this central term. Instead, the CCPA provides a nonexclusive list of practices that may qualify as discriminatory, such as:

- Denying goods or services to the consumer;
- Charging different prices or rates for goods or services;
- Providing a different quality of goods or services; and
- Suggesting that the consumer may receive a different price, rate, level, or quality of goods or services.

The CCPA further states, however, that a business may charge a consumer a different price or rate or provide a different level or quality of goods or services to the consumer if that difference is reasonably

[5] Virginia's approach to the Right to Opt Out is similar to the approach taken by Nevada. For further information on Nevada's law, see our article in Law360, Key Differences in Nev. And Calif. Data Privacy Laws.

related to the value provided to the business by the consumer's data and that a business may offer financial incentives as compensation for the collection, sale, or deletion of the consumer's personal information. The CPRA further clarifies that the anti-discrimination provision "does not prohibit a business from offering loyalty, rewards, premium features, discounts, or club card programs."

Like the CCPA, Virginia's CDPA also does not clearly define what constitutes discrimination. Instead the CDPA proscribes "processing personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers." It further prohibits a controller from discriminating against a consumer for exercising their CDPA rights, including by "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." The CDPA clarifies however that a controller is permitted to offer "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 the right to opt out or "the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program."

Right to an Appeal

While not necessarily a separate consumer right, the CDPA provides to consumers the right to appeal a data controller's refusal to take action on a consumer's request to exercise their other rights. The CDPA mandates that a "controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable time after the consumer's receipt of the decision." The right to appeal must be "conspicuously available" and similar to the process for submitting a consumer request to exercise the other personal information rights. Further, if the appeal is denied, the controller is required to provide the consumers with a method through which the consumer may contact the Virginia attorney general to submit a complaint. Neither the CCPA nor the CPRA contain a comparable obligation.

Contacts

Ron Raether
Partner
949.622.2722
ron.raether@
troutman.com

David Anthony
Partner
804.697.5410
david.anthony@
troutman.com

Ashley Taylor, Jr.
Partner
804.697.1286
ashley.taylor@
troutman.com

Wynter Deagle
Partner
858.509.6073
wynter.deagle@
troutman.com

Anne-Marie Dao
Associate
858.509.6057
anne-marie.dao@
troutman.com

Sadia Mirza
Associate
949.622.2786
sadia.mirza@
troutman.com

VCDPA Series: Part 3

Notice and Disclosure Obligations

One key area where Virginia's Consumer Data Protection Act (CDPA) differs from the California Consumer Privacy Act of 2018 (CCPA) and the California Privacy Rights Act of 2020 (CPRA)[1] is the law's notice and disclosure obligations.

In this third installment of our five-part series on Virginia's CDPA, we will review the contours of the law's notice and disclosure requirements, compare and contrast them with the requirements of California's CCPA and CPRA, and give helpful guidance to businesses seeking to ensure compliance with Virginia's new law.

As we explained in our prior installments, each of these privacy laws is based on the Fair Information Practice Principles (FIPPs), which include the principle that a consumer should be given notice of information practices before personal information is collected. However, each law differs in the kind, form, and extent of the notice that it obligates regulated entities to provide. The chart below previews how the Virginia and California laws differ with respect to these issues:

Obligations	CA CCPA	CA CPRA	VA CDPA
Privacy Policy	✓ Yes	✓ Yes	✓ Yes
Notice at Collection	✓ Yes	✓ Yes	✗ No
Notice of Right to Opt Out	✓ Yes	✓ Yes	✗ No
Notice of Financial Incentive	✓ Yes	✓ Yes	✗ No

These commonalities and distinctions are detailed further below.

A. The Notice/Disclosure Differences Between Virginia's CDPA and California's CCPA

The California CCPA imposes several notice and disclosure obligations on regulated businesses, derived from multiple interrelated, cross-referenced provisions of the law. These include:

1. Privacy Policy

A comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information, and the rights of consumers regarding their personal information.

2. Notice at Collection

A notice to provide consumer with timely notice, at or before the point of collection, about the categories of personal information to be collected from them, and the purposes for which the personal information will be used.

[1] The CPRA amended the CCPA in 2020. Except where specifically noted, both are referred to collectively as the CCPA hereafter.

3. Notice of Right to Opt Out

A notice to inform consumers of their right to direct a business that "sells" their personal information to stop selling their personal information.

4. Notice of Financial Incentive

A notice of the material terms of any financial incentives the business offers to consumers as compensation for the collection or sale of personal information (*e.g.*, coupons or special promotions that require sharing personal information for participation) so that the consumer may make an informed decision about whether to participate.

By contrast, the notice and disclosure requirements of Virginia's CDPA are *much* more streamlined and contained in a single section of the law titled, "Data controller responsibilities; transparency," § 59.1-574(C)-(E). In short, the Virginia CDPA requires only that a regulated "controller" provide a privacy notice to consumers, which includes certain listed information and, if applicable, a "clear and conspicuous" disclosure of the sale of personal information to third parties or use of personal information for targeted advertising and how the consumer may opt out of both.[2] This privacy notice requirement is most similar to the CCPA's "privacy policy" requirements. Notably, Virginia's CDPA *does not* require a separate notice at collection; does not require a separate notice of the right to opt out; and does not require notice of financial incentives.

The below breaks down the timing, form, and content of the privacy notice required by Virginia's CDPA.

B. Timing of Virginia CDPA Privacy Notice

Unlike the CCPA's "Notice at Collection" requirements, which require businesses to provide notice "at or before the point of collection," Virginia does not specify when the CDPA privacy notice must be provided to consumers. Rather, Virginia's CDPA simply requires controllers to provide consumers with a "reasonably accessible, clear, and meaningful" privacy notice, without specifying any timing requirements. That leaves the details of compliance somewhat open to interpretation, but suggests that Virginia's CDPA does not obligate controllers to provide a "just-in-time" notice. That is, there is no explicit requirement that Virginia's CDPA privacy notice be provided "at or before the point of collection."

C. Form of Virginia CDPA Privacy Notice

As noted above, Virginia's CDPA requires controllers to provide a privacy notice to consumers that is "reasonably accessible, clear, and meaningful." By comparison, the California CCPA requires a privacy policy "in a form that is reasonably accessible to consumers," and expressly specifies that for privacy policies provided online, the business will follow generally recognized industry standards, such as the World Wide Web Consortium's "Web Content Accessibility Guidelines," Version 2.1 of June 5, 2018. CCPA also requires the privacy policy to be posted online through a conspicuous link using the word "privacy" on the business's internet homepage or landing page of a mobile application, and instructs businesses that do not operate a website to make the privacy policy "conspicuously available to consumers."

The Virginia CDPA does not expand on what qualifies as "reasonably accessible, clear, and meaningful." Even in the absence of clarifying language, however, organizations should consider taking the following steps:

1. Avoid Legal Jargon

Use plain, straightforward language, avoiding technical or legal jargon.

[2] For information comparing a CCPA-regulated "business" to a CDPA-regulated "controller," see Part One of this series, which provides an introduction to and overview of the Virginia CDPA.

2. Adopt a Layered Format

Use a format that makes the notice readable, such as a layered format.

3. Post It Prominently and Use a Descriptive Title

Make the notice recognizable by giving it a descriptive title. In the case of a website, consider using a conspicuous link on your homepage containing the word "privacy." Make the link conspicuous by using larger type than the surrounding text and contrasting color symbols to call attention to it. Additionally, consider putting a conspicuous "privacy" link on every webpage where personal information is collected. In the case of an online service, such as a mobile application, consider posting or linking to the notice on the application's platform page, so that users can review the notice before downloading the application.

4. Option to Print

Format the notice so that it can be printed as a separate document.

5. Consider Readability

Use a format that makes the notice readable, including on smaller screens, such as on a mobile device.

6. Consider Alternative Means

For organizations that do not have a web presence, consider methods to inform consumers about how they can learn about your data collection and sharing practices.[3]

D. Content of Virginia CDPA Privacy Notice

Virginia's CDPA requires that a privacy notice include the following information:

1. The categories of personal data processed (CCPA refers to categories of data "collected" — there is likely no practical difference for the purpose of the privacy notice/privacy policy);
2. The purpose for which personal data is processed;
3. The way a consumer may exercise his or her rights under the CDPA, including how to appeal the controller's decision regarding a request to exercise them;
4. The categories of third parties the controller shares personal data with, and the categories of personal data shared with those third parties;
5. A description of one or more secure and reliable means for consumers to submit a request to exercise their consumer rights under the CDPA;[4] and
6. If the controller sells personal data to third parties or uses personal data for targeted advertising, a "clear and conspicuous" disclosure of that sale or use and the means to opt out. It is notable that the Virginia legislature chose to use the phrase "clearly and conspicuously" regarding the third-party sale and targeted advertising disclosure. The use of this language may suggest that this disclosure, where applicable, should be presented in a form distinguishable from the rest of the notice. This may be accomplished by using a bold or darker font, larger type, or a separate labelled section within the larger privacy notice.

[3] The guidance provided in this section is borrowed from the California attorney general's guidance on "Making Your Privacy Practices Public," which can be accessed here.

[4] Similar to the CCPA, Virginia's CDPA provides guidance as to what constitutes a "secure and reliable means," instructing businesses to consider (1) the ways a consumer normally interacts with the business, (2) the need for secure and reliable communication of the request, and (3) the ability to authenticate the identity of the consumer making a request.

Unlike California CCPA privacy policy requirements, the Virginia CDPA privacy notice does not need to include, among other things: (1) the sources from which personal data is collected; (2) a description of the process that will be used to verify consumer requests; (3) metrics on the number of consumer requests received, complied with, and denied in the previous calendar year; and (4) a description of a consumer's rights under the CDPA. With respect to the last point, however, the Virginia CDPA does require the privacy notice to describe "one or more secure and reliable means" for a consumer to request to exercise his or her rights, which may by implication warrant a disclosure of the rights available to a consumer under this law.

The following chart provides a high-level overview of the content requirements required by each law.

Items Required	CA CCPA	CA CPRA	VA CDPA
Categories of Data Collected/ Processed	✓ Yes	✓ Yes	✓ Yes
Sources from Which Data is Collected	✓ Yes	✓ Yes	✗ No
Purpose of Collection/Processing Data	✓ Yes	✓ Yes	✓ Yes
Categories of Data Shared with Third Parties	✓ Yes	✓ Yes	✓ Yes
Categories of Third Parties with Which Data is Shared	✓ Yes	✓ Yes	✓ Yes
Description of Consumer Rights	✓ Yes	✓ Yes	✗ No
Means to Exercise Consumer Rights	✓ Yes	✓ Yes	✓ Yes
Disclosure of "Selling" Practices and Method to Opt Out	✓ Yes	✓ Yes	✓ Yes
Disclosure of Targeted Advertising Practices and Method to Opt Out	✗ No	✓ Yes	✓ Yes
Description of the Process Used to Verify Consumer Requests	✓ Yes	✓ Yes	✗ No
Authorized Agent Instructions	✓ Yes	✓ Yes	✗ No
Metrics Relating to Number of Consumer Requests Received, Complied with, and Denied	✓ Yes	✓ Yes	✗ No
Date Last Updated	✓ Yes	✓ Yes	✗ No

E. The Infamous CCPA "Do Not Sell" Button

Another major difference between California's CCPA and Virginia's CDPA are the required notices regarding the sale or sharing of personal data with third parties, and the consumer's right to opt out of them. The California CCPA requires a business to include on its internet homepage a "clear and conspicuous link" enabling the consumer to opt out of the sale of the consumer's personal information to third parties (commonly referred to as a "Do Not Sell" button). The California CPRA expanded the scope of this requirement to include sharing of personal information with third parties for cross-context behavioral advertising (*i.e.*, a "Do Not Sell or Share" link).

On this subject, the Virginia CDPA does not require controllers to implement a "Do Not Sell" link on their internet homepages. Instead, a controller engaging in either (1) the sale of personal data to third

parties; or (2) the use of personal data for targeted advertising must disclose these practices and how a consumer may opt out. The provision requiring this disclosure provides no instructions as to the timing or format of this disclosure. Given its statutory location in between provisions relating to the privacy notice, however, and the lack of any other instruction as to where to post or when to provide it, this disclosure likely is intended to be included in the privacy notice.

F. A Path Forward

The California CCPA and Virginia's CDPA differ in many ways. Consumer notice and disclosure obligations are one area at least where Virginia's CDPA is notably more streamlined and straightforward.

On the other side of that same coin, however, the Virginia's CDPA provisions offer much less detail than the CCPA, leaving some important questions unanswered. Because the CDPA is based on the same core principles as other privacy laws (*i.e.*, the FIPPs), businesses would be doing themselves a disfavor if they did not consider how the notice and disclosure obligations included in other privacy laws — including California's CCPA — have been interpreted and enforced in the past. By doing so, many of the challenges organizations may face in implementing the Virginia CDPA privacy notice requirements may become less obscure, and organizations will be able to make compliance decisions that are informed, well-reasoned, and still in line with their business goals.

Contacts

Ron Raether
Partner
949.622.2722
ron.raether@
troutman.com

David Anthony
Partner
804.697.5410
david.anthony@
troutman.com

Ashley Taylor, Jr.
Partner
804.697.1286
ashley.taylor@
troutman.com

Jon Hubbard
Partner
804.697.1407
jon.hubbard@
troutman.com

Tim St. George
Partner
804.697.1254
tim.st.george@
troutman.com

Noah DiPasquale
Associate
804.697.1266
noah.dipasquale@
troutman.com

Sadia Mirza
Associate
949.622.2786
sadia.mirza@
troutman.com

VCDPA Series: Part 4

Data Processing Obligations

Identifying data processing obligations is tricky, especially as overlapping privacy laws are enacted. Compliance will always hinge on understanding what laws jurisdictionally apply and a firm grasp of the data collected and purpose of such collection. As discussed throughout this series, these related laws are generally rooted in the Fair Information Practice Principles (FIPPs), which serve as a reliable guidepost when developing a data privacy and security program.

The FIPPs provide, in part, that:

1. **Personal data should be relevant to the purposes for which they are used (Data Quality Principle);**
2. **The purposes for collecting personal data should be specified not later than at the time of data collection, and the subsequent use should be limited to fulfilling those purposes or others not incompatible with those purposes (Purpose Specification Principle); and**
3. **Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified (Use Limitation Principle).**

Despite being based on the same core principles, it is important to stay abreast of newly enacted comprehensive state privacy laws like the California Consumer Privacy Act (CCPA), and its recent amendments under the California Privacy Rights Act of 2020 (CPRA), and the Virginia Consumer Data Protection Act (CDPA), which include nuanced considerations that may differ on a jurisdictional basis and require specific actions based on such distinctions.

A. Data Minimization

Data minimization was not a core concept in the CCPA; however, it is a seminal component of other comprehensive data privacy laws like Europe's General Data Protection Regulation (GDPR). The principle of data minimization involves limiting data collection practices to what is required to fulfill a specific purpose. Both the CPRA and the CDPA incorporate this minimization concept to bar the collection of more personal information than necessary, as further detailed below.

Under the CPRA, personal and sensitive information collected must be "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed" and not be retained "longer than is reasonably necessary."

While Virginia's language is not phrased identically, it takes a similar approach and limits the collection of personal data to what is "adequate, relevant and reasonably necessary in relation to the purpose for which such data is processed, as disclosed to the consumer" and to "not process personal data for purposes not reasonably necessary or compatible with the disclosed purpose" unless the controller obtains the consumer's consent.

So what does data minimization practically require? For starters, under both the CPRA and CDPA, organizations must pay attention to their privacy notices and other consumer-facing disclosures and their disclosed "purposes for collection." This entails comprehensive data mapping and data classifications to understand what information is collected and how it is being used. Additionally, it is critical to have controls

in place to assure that data processing practices align with the disclosures and, if applicable, the consent provided by the consumer. Without careful planning, it would not be surprising to learn that the functionality of the product got ahead of the statements made in the privacy policy and other consumer-facing documents.

Other questions to consider when operationalizing data minimization requirements:

1. Does the personal information collected by the business have a rational link to the purposes for collection?

While data minimization is not explicitly included in the CCPA, the well-known "flashlight application" example included in the implementing regulations is relevant here. The example states that "if the business offers a flashlight application and the applications collects geolocation information, the business shall provide a just-in-time notice, such as through a pop-up window when the consumer opens the application … ." The notice should also explain the relationship between the data collected (*e.g.*, geolocation information) and the intended purpose (*e.g.*, address future enhancements or otherwise improve the flashlight functionality). Adequately disclosing data collection practices to consumers will enable businesses to set users' expectation of privacy and establish a defense to claims where plaintiffs to challenge the ultimate use of the information (*e.g.*, invasion of privacy and intrusion upon seclusion).

2. Has the business identified what personal information is necessary to fulfill its stated processing purposes?

In other words, collecting more personal information than is needed to achieve a particular purpose may not align with data minimization principles. Using the flashlight application as an example again, if certain data is being collected to improve the app's performance, then it may not make sense for the application to collect data when the application is not in use.

3. Does the business have a data retention/destruction policy in place to safely destroy personal information when no longer needed?

Unless privacy notices contemplate future business use, storing personal information on the off chance that it may be useful in the future may run afoul to data minimization requirements. Doing so also presents information security concerns and increases the risk in the event of a data breach. If retention of general information is important, consider implementing de-identification procedures to eliminate application of any statutory requirements. For data no longer required, it will also be important to consider proper data destruction and disposal methods.

B. Data Risk Assessments

Data risk assessments are not new — particularly related to sensitive personal data processed in electronic form. For instance, the Health Insurance Portability and Accountability Act (HIPAA) requires covered entities and their business associates to complete a thorough risk assessment to identify vulnerabilities that could result in a breach of protected health information. Similarly, the credit card industry's PCI-DSS requirements require entities that process and store electronic credit card data to perform and document risk assessments. Likewise, Massachusetts Standard for the Protection of Personal Information of Residents of the Commonwealth include a requirement to assess reasonably foreseeable internal and external risks to security of personal information. However, outside of specific laws, the U.S. generally does not require risk assessments be performed. This is changing, as evidenced by the CPRA and CDPA.

In contrast, Europe's GDPR requires data protection impact assessments when processing respective data will likely result in "a high risk to the rights and freedoms of natural persons."[1] While no similar requirement

[1] Recital 75 of the GDPR provides "[t]he risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result

existed under the CCPA, the new CPRA does empower the attorney general and the new California Privacy Protection Agency to possibly create similar risk assessment obligations. Similarly, Virginia's CDPA also includes risk assessment requirements, which are more concrete than corresponding CPRA provisions.

The following represents a basic summary of what processing practices require a risk assessment under the CCPA, CPRA, and CDPA:

Practices Requiring Risk Assessment	CA CCPA	CA CPRA	VA CDPA
Targeted Advertising	✗ No	✗ No	✓ Yes
Sale of Personal Data	✗ No	✗ No	✓ Yes
Processing of Sensitive Data	✗ No	✓ Yes*	✓ Yes
Profiling	✗ No	? Maybe*	✓ Yes
Heightened Risk of Harm	✗ No	✓ Yes*	✓ Yes

**Subject to upcoming attorney general regulations.*

The CPRA calls for a cyber audit to be conducted whenever processing personal information may pose a significant risk to the privacy or security of a consumer's personal information.[2] The goal of these assessments is to determine if the risks to the consumer outweigh the benefits.[3] Additionally, the CPRA allows the newly created Consumer Privacy Protection Agency to require businesses to submit such risk assessments for review on a "regular basis."[4]

Unlike the CPRA, the CDPA has more specific language as to when a risk assessment must be performed. These activities include targeted advertising, the sale of personal data, processing of sensitive data, specific instances of involving profiling, and where such processing poses a heightened risk of harm to consumers.[5] Regardless of these differences, both laws articulate the same goal (using nearly identical language): Risk assessments are intended to identify and weigh the benefits that may flow from such processing to the business, consumer, other stakeholders, and the public.

The requirements for risk assessments under Virginia's CDPA do not take effect until January 1, 2023; moreover, to the extent assessments are performed in compliance with other comparable laws, such assessment may comply under the CDPA.[6] Regardless, companies should begin to prepare now, and consider how internal processes need to change, as well as the privilege and litigation issues that may arise as a result of creating these reports.

from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects. "risks to the rights and freedoms of natural persons."

[2] CCPA § 1798.185(a)(15).
[3] CCPA § 1798.185(a)(15)(B).
[4] CCPA § 1798.185(a)(15)(B).
[5] CDPA § 59.1-576(A)(1)-(5).
[6] CDPA §59.1-576(D)-(E).

C. Specific Processing Requirements for Unique Data Types

New privacy laws, like those in California and Virginia, highlight the importance of data mapping to adequately identify when collecting and processing certain types of data trigger unique requirements. For example, both California and Virginia include opt-out requirements that are triggered when information is used for particular purposes (*e.g.*, "selling" personal information). Likewise, California and Virginia also include specific opt-in requirements when certain types of data are at issue (*e.g.*, "sensitive data" or data belonging to children). Without proper data mapping and classification in place, businesses may not be able to identify when specific requirements are triggered.

The following is a basic summary of explicit opt-out requirements under the CCPA, CPRA, and CDPA:

Opt-Out Required	CA CCPA	CA CPRA	VA CDPA
Targeted Ads	✗ No	✓ Yes*	✓ Yes
"Sale" of Personal Information	✓ Yes	✓ Yes	✓ Yes
Profiling	✗ No	✗ No**	✓ Yes

**The CPRA provides a new right to opt out of sharing of personal information. Sharing (a new term under the CPRA) refers to providing personal information to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration.*
***Regulations will need to be developed governing access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in such decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer (CPRA § 1798.185 (a)(16)).*

Sensitive Information

The concept that certain information is more "sensitive" than others does not exist under California's CCPA. The CPRA amended this, however, with its definition of "sensitive personal information," which means personal information that reveals:

- A consumer's Social Security, driver's license, state identification card, or passport number;
- A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
- A consumer's precise geolocation;
- A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;
- The contents of consumer's mail, email, and text messages, unless the business is the intended recipient of the communication; and
- A consumer's genetic data.

"Sensitive personal information" under the CPRA also includes:

- The processing of biometric information for the purpose of uniquely identifying a consumer;
- Personal information collected and analyzed concerning a consumer's health; and
- Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.[7]

[7] It is worth noting that California's CPRA definition of "sensitive personal information" is broader than California's definition of "personally identifiable information," which triggers California's data breach notification requirement and are outlined in Cal. Civ. Code § 1798.82. In other words, the unauthorized disclosure of "sensitive personal information," as defined by the CPRA, may not be sufficient to trigger California's data breach notification requirements.

Under Virginia's CDPA, "sensitive data" is more narrowly defined to include only the following:

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

Under the CPRA, consumers must be able to limit the processing of sensitive personal information. This is effectively a scalable opt out. Alternatively, Virginia's CDPA prohibits the processing of sensitive data without obtaining the consumer's consent — inherently an opt-in requirement. Below is a basic chart outlining these requirements.

Treatment of Sensitive Information	CA CCPA	CA CPRA	VA CDPA
Opt-Out Consent	✗ No	✓ Yes	✗ No
Opt-In Consent	✗ No	✗ No	✓ Yes

While there is overlap between the respective laws' definitions, there are noticeable differences. Companies engaged in business across jurisdictions must be considerate of these distinctions and subsequent associated requirements. In particular, with California and Virginia each tying risk assessments requirements to certain processing of sensitive information, understanding what information is collected and when it may be deemed sensitive is even more important.

Children Information

Children's and youth data are generally treated with more care under privacy regimes. Indeed, there is normally a heightened standard for consent, particularly for children under 13 who may not be mature enough to provide such consent, and instead, a parent or guardian must be informed and provide such consent. This concept has been codified in the Children's Online Privacy Protection Act (COPPA).

The CCPA and CPRA go a step further than COPPA. In California, the law distinguishes between children under 13 years old and children between 13 and 16 years old. In the case of children under 13, the parent or guardian must affirmatively authorize the "sale" of the child's personal information. In contrast, children between 13 and 16 can opt in on their own behalf. In both cases, the consent requirement is an opt-in consent meaning that the child's personal information cannot be "sold" unless the parent or child (depending on the age of the child) affirmatively authorizes the sale. Moreover, these requirements are "in addition to any verifiable parental consent required under COPPA."[8]

Virginia, on the other hand, takes a simpler approach with respect to children. Under the CDPA, the law only addresses children younger than 13 years of age and requires any related processing (including consent requirements) to be performed in accordance with COPPA.[9]

[8] California Attorney General Regulations to the CCPA, 11 CA ADC § 999.330(a).
[9] CDPA § 59.1-574(A)(5); CDPA § 59.1-572(D).

D. Vendor Contract Requirements

A common requirement of omnibus type privacy laws concerns entities — downstream of the entity with the consumer relationship — processing personal information on behalf of a company. Laws will use different terminology to describe such entities — some described as a "service provider" like in the CCPA or "contractor" under the CPRA's updated revisions. Other laws use terms like "processor" (similar to the GDPR). Regardless of the name, the main purpose of related provisions is to ensure contractual protections exist to limit how downstream entities can process personal information.

CCPA "Service Providers"

Under the California's CCPA, a "service provider" is any (1) for-profit entity that (2) processes information on behalf of a business that (3) receives personal information from the business for a business purpose (4) pursuant to a written contract that prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any other purpose. Thus, for an entity to qualify as a service provider, all four elements arguably must be met.[10]

CPRA "Contractors"

In addition to "service providers," California's CPRA includes the concept of "contractors." Contractors are essentially the same as service providers in the sense that they are persons who receive personal information from a business, pursuant to a written contract, which limits how such information can be retained, used, or disclosed. While not explicitly clear, the difference between a "service provider" and "contractor" likely depends on the purpose for which personal information is disclosed, with service providers being those innately involved in "processing" personal information, and contractors being those who may inadvertently receive personal information as part of the services they provide.

Likely to prompt yet another round of reviews and updates to contracts, the CPRA requires contracts with services providers and contactors to include, among other things, the following:

- Language prohibiting combining personal information received from a business with personal information collected through other means;
- An obligation to comply with applicable obligations under the CPRA and provide the same level of privacy protection as required by the CPRA (in contrast to the CCPA, where service providers obligations are imposed only through contract);
- The right of the business to take reasonable and appropriate steps to ensure personal information shared is used in a manner consistent with the business's obligations under the CPRA and the right to, upon notice, take reasonable and appropriate steps to stop and remediate unauthorized use of personal information; and
- An obligation to notify the business if the entity determines it can no longer meet its obligations under the CPRA.

The CPRA also requires service providers and contractors who engage any other person to assist in processing personal information (*i.e.*, a subcontractor or sub-service provider) to notify the business of such engagement. This notification requirement also extends to situations where persons engaged by the service provider of a contractor engage another person, effectively requiring service providers and contractors to notify a business of any subcontractor or a sub-service provider relationship at least two tiers below the business.

[10] For additional information on vendor requirements under California's CCPA, see our *Law360* article, "Calif. Privacy Law Means New Approach to Vendor Contracts."

CDPA "Processors"

Virginia's privacy law, alternatively, focuses on "processors." A "processor" is simply a "natural or legal entity that processes personal data on behalf of a controller." To qualify as a processor, the contract between a controller and a processor must set forth (i) the instructions with respect to processing, (ii) nature and purpose of the processing, (iii) type of data subject related to the processing, (iv) duration of processing, and (v) "the rights and obligations of both parties." This approach is more similar to that of the GDPR than the CCPA. The contract must also include requirements that the processor:

- Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;
- 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;
- 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 its obligations;
- 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 its obligations using an appropriate and accepted control standard or framework and assessment procedure for such assessments; and
- Engage any subcontractor pursuant to a written contract to meet the obligations of the processor with respect to the personal data.

Below is a high-level chart that compares the respective written contract requirements with downstream entities under the CCPA, CPRA, and CDPA:

Contract Requirements	CA CCPA	CA CPRA	VA CDPA
Explicit Prohibition on Selling PI	✓ Yes	✓ Yes	✗ No
Explicit Prohibition on Sharing PI	✗ No	✓ Yes	✗ No
Explicit Prohibition on Processing Outside the Business Purpose Specified in the Contract	✓ Yes	✓ Yes	✗ No
Explicit Prohibition on Combining Personal Information with Other Personal Information from Other Sources Outside the Business Purpose	✗ No	✓ Yes	✗ No
Instructions for Processing	✗ No	✗ No	✓ Yes
Nature and Purpose of Processing	Not explicitly required, but recommended to include the "business purpose" for processing PI	✗ No	✓ Yes

Contract Requirements	CA CCPA	CA CPRA	VA CDPA
Type of Data Subject Related to the Processing	✗ No	✗ No	✓ Yes
Processing Duration	✗ No	✗ No	✓ Yes
Rights and Obligations of Both Parties	✗ No	✗ No	✓ Yes
Duty of Confidentiality	✗ No	✗ No	✓ Yes
Return of Confidential Information	✗ No	✗ No	✓ Yes
Provide Information Demonstrating Compliance	✗ No	✓ Yes*	✓ Yes
Reasonable Audits	✗ No	✓ Yes*	✓ Yes

**Contract may permit the business to monitor the vendor's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.*

In practice, both approaches will effectively limit the scope of processing allowed by any downstream entity. However, to the extent both jurisdictions apply, it will be important to consider the phrasing of any written agreement requirements to ensure that all of the respective points are met. As more states adopt similar omnibus approaches to data privacy and security, allowing for a streamlined process to update data processing agreements to reflect written contract requirements will be important to not only maintain a compliant program, but also a manageable contract life cycle management program.[11]

Contacts

Ron Raether
Partner
949.622.2722
ron.raether@
troutman.com

David Anthony
Partner
804.697.5410
david.anthony@
troutman.com

Ashley Taylor, Jr.
Partner
804.697.1286
ashley.taylor@
troutman.com

Brett Dorman
Associate
949.567.3541
brett.dorman@
troutman.com

Sadia Mirza
Associate
949.622.2786
sadia.mirza@
troutman.com

[11] Troutman Pepper has a dynamic and proven contract life cycle management practice. We advise clients of all types in implementing best practices, processes, personnel realignment and technology solutions to efficiently and systematically manage contract creation, execution, negotiation, implementation, performance, analysis, review, storage, reporting and compliance. For additional information on our Commercial Contracting practice, click here.

VCDPA Series: Part 5

Litigation and Enforcement

Like the California Consumer Privacy Act of 2018 (CCPA) and the California Privacy Rights Act of 2020 (CPRA), the Virginia Consumer Data Protection Act (VCDPA) does not grant a private right of action for alleged violations of its obligations. Rather, enforcement of the VCDPA is the exclusive province of the attorney general (AG) of Virginia.

All Fair Information Practice Principles (FIPPs) state that organizations should be accountable for complying with the measures that give effect to the other principles we've discussed throughout this series (*e.g.,* data quality, purpose specification, use limitation, individual participation, etc.). In this fifth and final installment of our series on the VCDPA, we review the ways in which the VCDPA will be enforced, both inside and outside of court. We also compare Virginia's enforcement mechanisms with California's and give helpful compliance guidance to businesses that will be governed by Virginia's new law.

The following chart compares the Virginia and California laws:

Litigation and Enforcement	CCPA	CPRA	VCDPA
Private Right of Action for Violations of the Act	✗ No	✗ No	✗ No
Private Right of Action for Data Breaches	✓ Yes	✓ Yes	✗ No
Cure Period	✓ Yes	✓ Yes	N/A
AG Enforcement Action	✓ Yes	✓ Yes	✓ Yes
Cure Period	✓ Yes	Discretionary	✓ Yes
Agency Enforcement Action	✗ No	✓ Yes	✗ No
Cure Period	N/A	Discretionary	N/A
Effective Date	Jan. 1, 2020	Jan. 1, 2023	Jan. 1, 2023
Enforcement Date	July 1, 2020	July 1, 2023	Jan. 1, 2023
Retroactive	✗ No	✗ No	✗ No
Requirement to Adopt Implementing Regulations	✓ Yes	✓ Yes	✗ No

These similarities and differences are explained below.

A. Private Rights of Action

While neither the CCPA[1] nor the VCDPA provide for a private right of action, the statutes differ as the CCPA allows consumers to recover damages if a business' violation of the duty to implement and maintain reasonable security procedures results in a data breach. There is no private right of action under the

[1] The CPRA amended the CCPA in 2020. Except where specifically noted, both are referred to collectively as the CCPA hereafter.

VCDPA, not even for data breaches.

Also, under the CCPA, consumers must provide a business with a 30-day written notice and cannot sue if the violation is cured during that period. If the violation is not cured during that period, the consumer may recover (1) the greater of actual damages or statutory damages ($100 to $750) per consumer per incident, (2) injunctive or declaratory relief, and (3) any other relief the court deems proper.

B. Government Actions

1. AG Enforcement Authority

Under the CCPA and VCDPA, the AG has exclusive enforcement authority. This will change in California once the CPRA takes effect and creates the California Privacy Protection Agency, a five-member board that has the authority to (1) investigate possible violations of the CPRA upon the sworn complaint of any person or on its own initiative and (2) bring an administrative action to enforce violations. Virginia has no similar enforcement agency.

2. Cure Periods

Although the CCPA currently requires the AG to provide a 30-day cure period before suing, the CPRA removes that requirement and grants the AG discretion whether to provide a cure period. The VCDPA, in contrast, requires the AG to provide a 30-day cure period and bars AG action if a business successfully cures its violation. This cure period effectively limits enforcement in Virginia to alleged violations after the business has had an opportunity to cure. Accordingly, enforcement actions cannot be brought for any violations that are cured during the cure period — regardless of any damage already done.

3. Penalties

Once the CPRA takes effect, the California Privacy Protection Agency or the California AG may recover up to $2,500 for each violation or up to $7,500 for each intentional violation or violations involving the personal information of a minor consumer.

In Virginia, the Virginia AG may recover a civil penalty of up to $7,500 per violation. The Virginia AG may also recover reasonable expenses incurred in investigating and preparing the case, including attorney fees.

C. Implementing Regulations

Another difference involves implementing regulations. The CCPA required the California AG to create implementing regulations. The CPRA requires additional regulations to be adopted by July 1, 2022.[2] The VCDPA, by contrast, does not require any implementing regulations.

D. Retroactivity

A recent opinion from the U.S. District Court for the Northern District of California held that the CCPA does not apply retroactively, meaning it is limited to alleged violations that occurred after January 1, 2020, when it became effective.[3] Because "Virginia law does not favor retroactive application of statutes," and the VCDPA does not contain a "manifest" statement that the legislature intended it to apply retroactively, enforcement should be limited to violations that occur after the statute becomes effective on January 1, 2023.[4]

[2] The California Privacy Protection Agency can assume authority to issue these regulations by providing the California AG with notice.

[3] Order Granting Motion to Dismiss and Denying Motion to Strike Class Allegations, *Gardiner v. Walmart, Inc.*, No. 4:20-cv-04618 (N.D. Cal. Mar. 5, 2021), ECF No. 43.

[4] *Bailey v. Spangler*, 289 Va. 353, 358–59 (2015).

E. Consumer Privacy Funds

Both California and Virginia created funds in their state treasuries called the "Consumer Privacy Fund."

In California, the Consumer Privacy Fund was created to house the proceeds of any settlement of an action brought pursuant to the CCPA. Funds transferred to the Consumer Privacy Fund are used first to offset any costs incurred by the state courts and the AG in connection with the CCPA, and then 91% invested by the treasurer and 9% to the California Privacy Protection Agency for the purposes of creating grants in California. The California Consumer Privacy Fund was initially funded through the General Fund with $5,000,000 during the fiscal year 2020-2021, and $10,000,000 during each fiscal year thereafter.

The VCDPA created a special non-reverting fund known as the Consumer Privacy Fund that is used to support the work of the Virginia AG to enforce the VCDPA, subject to appropriation. All civil penalties collected under the VCDPA are paid into the state treasury and credited to the fund.

F. Predicted Enforcement Impact

According to the Virginia AG, its enforcement obligations under the VCDPA will require it to spend $330,556 per year to hire a dispute resolution specialist, a consumer protection investigator, and an assistant AG to handle additional individual consumer complaints, and, where deemed appropriate, pursue actions on behalf of those consumers.[5] Although the Virginia AG has stated that it does not expect recoveries from civil penalties to be sufficient to cover these personnel costs, it is unclear if that is simply because enforcement will not be possible until January 1, 2023, or because the office does not expect recoveries to exceed $330,556 after that date. Nevertheless, businesses should not assume that enforcement actions will not be a priority starting in 2023. Businesses should prepare for immediate enforcement and develop strong compliance programs ahead of 2023.

Given the similarities between the CCPA and VCDPA, businesses should keep an eye on the issues that may give rise to enforcement actions under the CCPA as those issues will likely be on the Virginia AG's radar as well. For further information on areas of enforcement likely to catch the California AG's attention, see our California Consumer Privacy Act Enforcement Series, available here.

Contacts

Ron Raether
Partner
949.622.2722
ron.raether@
troutman.com

David Anthony
Partner
804.697.5410
david.anthony@
troutman.com

Ashley Taylor, Jr.
Partner
804.697.1286
ashley.taylor@
troutman.com

Ketan Bhirud
Counsel
202.274.2890
ketan.bhirud@
troutman.com

Justin Golart
Associate
804.697.1477
justin.golart@
troutman.com

Julie Hoffmeister
Associate
804.697.1448
julie.hoffmeister@
troutman.com

Sadia Mirza
Associate
949.622.2786
sadia.mirza@
troutman.com

[5] https://lis.virginia.gov/cgi-bin/legp604.exe?211+oth+SB1392FES1122+PDF