Articles + Publications | March 25, 2021

Data Processing Obligations: Virginia Consumer Data Protection Act Series (Part Four)

WRITTEN BY

Ronald Raether, Jr. | David N. Anthony | Ashley L. Taylor, Jr. | Sadia Mirza | Brett A. Dorman

Download PDF

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 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:

**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.

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:

**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]

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.

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]

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.

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 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]

---

[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 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).

[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.

[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).

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

[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.

RELATED INDUSTRIES + PRACTICES

- Consumer Financial Services
- Privacy + Cyber
- State Attorneys General