Baker McKenzie.

October 2022

United States: Comparing the Colorado Privacy Act with the California Consumer Privacy Act

In brief

Contents

Who and what data are protected?

Who must comply?

How to comply?

Sanctions and remedies

Businesses that have implemented measures to comply with the California Consumer Privacy Act of 2018, as amended by the California Consumer Rights Act of 2020 (CCPA) can leverage some of their existing vendor contract terms, website disclosures and data subject rights response processes to satisfy requirements under the Colorado Privacy Act (**CPA**). However, the CPA, and the recently published proposed CPA Rules, (located here), contain certain unique and prescriptive requirements that may warrant taking a CPA-specific approach to compliance. How the finalized CCPA regulations and CPA Rules look will largely dictate whether companies will need to expand or change the scope of their privacy compliance measures to meet the obligations set forth under both California's and Colorado's privacy regimes.

Who and what data are protected?

The CPA protects "consumers", which the statute defines as Colorado residents acting in an individual or household context. Individuals acting in an employment or commercial context are expressly excluded from protection. Protected information under the CPA includes information that is linked or reasonably linkable to an identified or identifiable individual, but does not include such data that is de-identified or publicly available.

The CPA includes exemptions for certain types of data and entities. These include exemptions for air carriers and certain financial institutions governed by the Gramm-Leach-Bliley Act (GLBA) and certain data maintained by a public utility, employment records, protected health information processed by covered entities and business associates under the Health Insurance Portability and Accountability Act (HIPAA), and other types of information already regulated under other federal laws, including the GLBA, Family Educational Rights and Privacy Act (FERPA), Fair Credit Reporting Act (FCRA), and Children's Online Privacy Protection Act (COPPA).

Who must comply?

Unless an exemption applies, the CPA applies to "controllers" and "processors" that conduct business in Colorado or sell products or services intentionally targeted to residents of Colorado, **and** meet either of the following thresholds: the business (i) controls or processes personal data of 100,000 or more consumers during a calendar year; or (ii) derives revenue or receives discounts from the sale of personal data and controls or processes data of at least 25,000 consumers. Notably, and unlike the CCPA, and other state privacy laws becoming operative in 2023, the CPA applies to non-profit entities.

"Controller" is analogous to a "business" under the CCPA and is defined as a person that, alone or jointly with others, determines the purposes for and means of processing personal data. "Processor" is analogous to a "service provider" under the CCPA and is defined as a person who processes personal data on behalf of a controller. To qualify as a "processor" under the CPA, a company has to process personal data on behalf of a controller. The CPA mandates that processors adhere to the controller's instructions and assist the controller to comply with the controller's own obligations, and the two parties must enter into an agreement with certain terms prescribed by the CPA. Under the

CCPA, to qualify as a "service provider" a company must both enter into and adhere to a contract with certain terms and only process personal information for certain business purposes as defined by the CCPA.

How to comply?

Privacy Notices. *Under the CPA,* controllers must provide privacy notices that include: (i) the data categories collected or processed; (ii) the purposes for which the categories are processed; (iii) how and where consumers may exercise their rights, including the controller's contact information and how a consumer may appeal a controller's action with regard to a consumer's request; and (iv) categories of data shared with third parties. Most of these notice obligations are similar to obligations under the CCPA, except for the requirement to disclose Colorado-specific processes to appeal a controller's request-related action.

Moreover, controllers that "sell" personal data, or that process personal data for targeted advertising, must disclose the sale or processing and the manner in which a consumer may exercise the right to opt-out of the sale or processing. The CPA defines a "sale" of data in a similar manner as the CCPA as an exchange of personal data for monetary or other valuable consideration by a controller to a third party. This means that transferring personal data for something valuable alone constitutes a sale, and a party need not receive money in return for the personal data to have been considered "selling" the data. However, the CPA excludes certain types of disclosures from being a "sale" of personal data, such as disclosures to a processor to process the data for the controller, of personal data to a third party for the purpose of providing a product or service requested by the consumer, to an affiliate of a controller, to third parties in relation to a merger or similar transaction, that a consumer directs the controller to disclose, or of data intentionally made available by a consumer to the general public.

The recently published draft CPA Rules, however, include more prescriptive notice requirements. For example, they prescribe how controllers must post privacy notices when operating online (e.g., using a link with the word "privacy" on a controller's website - as also required by the currently operative CCPA regulations) or offline (e.g., distributing an offline notice to consumers through a medium regularly used by the controller to interact with consumers). They also require notices to include detailed explanations of how consumers can exercise their data privacy rights under the CPA. Notably, and in contrast with the common structure of CCPA privacy notices, under the draft CPA Rules, controllers would need to identify processing purposes and, for each purpose, note which personal data categories are processed for such purpose. In addition, any changes to a company's notice will require at least 15 days' notice to consumers under the proposed CPA rules.

Loyalty Program Disclosures. Similar to the CCPA's obligation to issue a notice of "financial incentive" where a business offers special programs or services in exchange for personal information, the proposed CPA Rules require loyalty program-related disclosures. The requirements, however, are generally less burdensome than those that apply to CCPA notices of financial incentives (e.g., there is no need to explain the method used to calculate the value of data, or analyze how such value is reasonably related to the value provided by the loyalty program).

Technical and Organizational Measures, Assessments, and Data Processing Agreements. The CCPA requires controllers to establish, implement, and maintain reasonable administrative, technical and physical data security practices, and to conduct and document data protection assessments before engaging in any processing activity that presents a heightened risk of harm to a consumer. The CPA considers processing for purposes of targeted advertising or profiling, selling personal data, and processing sensitive data to be activities that typically present a heightened risk of harm to consumers. The CCPA did not initially contain such an assessment requirement, but the California Privacy Protection Agency is tasked under the CCPA to issue regulations that will require audits and risk assessments as well. The proposed CPA Rules set out 18 different items that must be covered in a privacy risk assessment, and enumerates certain risks that must be accounted for. Depending on how the finalized CPA Rules and CCPA Regulations look, companies may be able to leverage assessments to comply with both privacy regimes.

Further, before a processor performs any processing on behalf of a controller, the parties must enter into a contract that includes terms similar to those required under other state privacy laws, including controller-to-processor instructions, provisions on the types of processed data and their retention periods, and confidentiality commitments. Data processors must adhere to controllers' instructions and use appropriate technical and organizational measures to assist controllers in meeting their obligations under the CPA.

Data Subject Rights. Under the CPA, consumers have the right to know whether a controller is collecting their personal data, to access their collected personal data, to download and remove personal data from a platform in a format that allows the transfer to another, and to correct and delete personal data held on them. Consumers also have the right to opt out of the sale of their personal data, or use of their personal data for targeted advertising and certain types of profiling. Notably, controllers must offer a universal opt-out tool by 1 July, 2024.

Obtaining Consumer Consent. Both the CCPA and CPA include some circumstances that require a controller to obtain consent from consumers. However, under the proposed CPA Rules, Colorado introduced an explicit concept of "refreshing consent." The CPA Rules state that a controller must refresh consent "at regular intervals," although the only additional rule on what constitutes a "regular interval" is that a controller should consider the context and scope of the original consent, the sensitivity of the personal data at issue, and the reasonable expectations of the consumer. The CPA Rules also explicitly require controllers to obtain new consent when a processing purpose changes, such that the new purpose is a secondary use of the collected personal information. This is different from the draft amendments to the CCPA regulations and their requirement that businesses obtain up front explicit consumer consent to collect personal data where the collection, use or retention of that personal data is not necessary or proportionate or is unrelated or incompatible with the established collection purposes.

Universal Opt-Out Mechanism. Similar to the currently operative CCPA regulations, the CPA contemplates that consumers will have the right to opt-out of sales of their personal data and targeted advertising by activating a universal opt-out mechanism. The CPA provides that the Colorado Attorney General will establish the technical specifications of such universal opt-out mechanisms, and the proposed CPA Rules sets forth detailed requirements on how such mechanisms must operate. The proposed CPA Rules also state that the Colorado Department of Law will release an initial list of acceptable technologies considered to meet its "universal opt-out" mechanism standards by 1 April, 2024. Companies that sell Colorado residents' personal data or engage in targeted advertising will have to use technologies enumerated on the state's list of approved universal opt-out mechanisms to comply with the CPA.

Timelines for Responding to Data Subject Rights Requests*.* To exercise one's rights, the CPA allows consumers to, once they have been authenticated, receive responses to consumer requests within 45 days. Controllers may extend this time period by another 45 days where reasonably necessary, and the consumer will ultimately have the ability to appeal any decision made by the controller under the controller's appeal process (which is mandated by the CPA). The appeals process must provide the consumer with an appellate response within 45 days (which can be extended by another 60 days if reasonably necessary), and must end with the consumer's ability to contact the Colorado attorney general if the consumer has concerns about the results of any appeal. This contrasts with the CCPA, which does not mandate an appeals process.

Sensitive Data. The CPA defines "sensitive data" to mean certain prescribed categories of data, including personal data that reveals an individual's race, ethnic origin, religious beliefs, mental or physical health conditions or diagnoses, sexual activity, orientation or preferences, citizenship status, as well as personal data from a known child (under 13) and biometric information. The proposed CPA rules also creates a new category of sensitive data titled "Sensitive Data Inferences." Accordingly, inferences made from data that concern the enumerates sensitive data categories are also subject to additional requirements and limitations.

Unlike the CCPA, which will introduce an "opt-out" regime for the processing of sensitive personal information beyond certain authorized purposes, the CPA requires controllers to obtain consumers' consent before processing their sensitive data. Thus, Colorado's sensitive data-related obligations are generally more burdensome than those in California, although this is counterbalanced by the fact that the definition of sensitive data is more limited under the CPA than under the CCPA.

Sanctions and remedies

There is no private right of action provided by the CPA, but the Colorado attorney general or Colorado district attorneys can bring a civil action for an injunction or penalties. The law does not issue guidance on fines, but instead states that a CPA violation is a deceptive trade practice, which would in turn impact a civil action asserting a claim under the Colorado Consumer Protection Act. An entity violating the CPA could therefore be subject to a fine of USD 20,000 per violation. Until 1 January 2025, the Colorado attorney general or Colorado district attorneys must first, if an offense is curable, issue a notice of violation to a controller and allow a 60-day cure period before pursuing an enforcement action.

Contact Us

Lothar Determann
Partner
lothar.determann@bakermckenzie.com

Helena Engfleldt
Partner
helena.englfeldt@bakermckenzie.com

Jonathan Tam
Partner
jonathan.tam@bakermckenzie.com

Tom Tysowksy
Associate
tom.tysowksy@bakermckenzie.com

Ownership: This site (Site) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms, including Baker & McKenzie LLP). Use of this site does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All information on this Site is of general comment and for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulation and practice are subject to change. The information on this Site is not offered as legal or any other advice on any particular matter, whether it be legal, procedural or otherwise. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any information provided in this Site. Baker McKenzie, the editors and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents of this Site. **Attorney Advertising:** This Site may qualify as "Attorney Advertising" requiring notice in some jurisdictions. To the extent that this Site may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME.