Colorado Privacy Act Overview

***By: Camila Tobón*[1]**

Colorado has become the third state to pass comprehensive privacy legislation, following Governor Jared Polis's signing into law of the Colorado Privacy Act ("CPA") this summer. The CPA is more like the Virginia Consumer Data Protection Act ("VCDPA"), which was enacted in March of this year, than the California Consumer Privacy Act ("CCPA"), which was enacted in 2018 and took effect on January 1, 2020. Nevertheless, there are common themes across the three laws, the most salient of which are accountability and consumer control. Notably, these themes also appear in the numerous other proposals considered through the U.S. states this year, indicating that U.S. regulation of personal information is evolving. Whereas prior regulation focused on particular data sets and potential harm to consumers from misuse or unauthorized use of such data, recent frameworks focus on giving individuals control over their data and holding companies accountable for what they choose to do with the personal data they collect. This evolution from a harms-based approach to a rights-based approach will put the onus on companies to understand what personal information they have, how they use it, and with whom they share it.

The CPA's Scope

The CPA takes effect on July 1, 2023 and applies to companies that collect and process the personal data of "consumers." A consumer is an individual who is a Colorado resident acting only in an individual or household context. The term does not include an individual acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context. Personal data is broadly defined as information that is linked or reasonably linkable to an identified or identifiable individual. A subset of personal data, called sensitive, is given heightened protections. Sensitive personal data includes data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status.

Covered entities include companies that conduct business in Colorado or produce products or services targeted to residents of the state and that either (i) handle the personal data of at least 100,000 consumers per calendar year or (ii) derive revenue or receive a discount on the price of goods or services from the sale of personal data and process the personal data of at least 25,000 consumers.

These thresholds for applicability largely track those found in the VCDPA. The CCPA uses different thresholds altogether, focusing on annual revenue ($25 million annually) or sales revenue (at least 50% from the sale of personal information) as well as volume of sales (sales of personal information about 50,000 consumers, households or devices, which will change to 100,000 consumers or households in 2023).

Exceptions to the CPA's scope include both entity-level and data-level exceptions. Entity-level exceptions exist for financial institutions or affiliates subject to the federal Gramm-Leach-Bliley Act (GLBA) and air carriers. Data-level exceptions include data maintained for employment records

---

[1] Ms. Tobón is a partner in the Denver office of Shook, Hardy & Bacon. She assists clients with data protection compliance, privacy and data security risk management, and information governance. She holds certifications in EU and U.S. privacy law and privacy program management and is a designated Fellow in Information Privacy and Privacy Law Specialist by the International Association of Privacy Professionals.

purposes; data about individuals acting in a commercial or employment context, job applicants, and beneficiaries of someone acting in an employment context; and data subject to certain federal laws (e.g., the Health Information Portability and Accountability Act, the Fair Credit Reporting Act, the Children's Online Privacy Protection Act, and the Family Education Rights and Privacy Act). Notably, the CPA does not exempt non-profit organizations, which differs from the CCPA and VCDPA.

CPA Consumer Rights

The CPA gives consumers the following rights:

- The right to opt-out of targeted advertising, sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer. Note that beginning July 1, 2024 this must include the ability to opt out of targeted advertising or sale through a universal opt-out mechanism;
- The right to access and port personal data;
- The right to correct inaccurate personal data;
- The right to delete;
- The right to opt-in to the processing of sensitive personal data.

These rights largely track the rights given to consumers by the VCDPA. However, there are a few differences between these rights and those available in the CCPA. For example, the right to opt-out in the CCPA is narrower while the right to access is broader. In California, the opt-out applies only to the sale of personal data and, beginning in 2023, to the sharing of personal data for targeted advertising. The right to access has two parts under the CCPA, one relating to the categories of personal information collected and the other relating to the specific pieces collected. And the right to correct does not yet apply. It kicks in when the California Privacy Rights Act ("CPRA"), which amends the CCPA, takes effect on January 1, 2023. Lastly, the CCPA/CPRA rights will apply to employee and commercial personal data beginning January 1, 2023 unless the current exemptions are extended.

Controller Obligations

The CPA defines "controller" as the entity that, alone or jointly with others, determines the purposes and means of processing personal data. Controllers must satisfy the following obligations:

- Provide consumers with a reasonably accessible, clear, and meaningful privacy notice;
- Specify the express purpose for which personal data will be collected and processed;
- Collect personal data that is adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes;
- Avoid secondary uses of personal data that are not reasonably necessary or compatible with the specified purposes, unless consent is first obtained;
- Take reasonable measures to secure personal data;
- Avoid processing personal data in violation of state or federal laws that prohibit unlawful discrimination;
- Conduct data protection impact assessments of "high risk" processing activities (including, targeted advertising, profiling, sale, and sensitive data processing);
- Enter into data processing agreements with processors/service providers.

These requirements track the VCDPA, except that the VCDPA gives the controller discretion to identify other processing activities that may pose a "heightened risk of harm" to consumers and complete a risk assessment for those. As compared to California, the CPRA will introduce many of these controller requirements (to "businesses," which is the CCPA/CPRA defined term), such as proportionality; agreements with third parties, service providers, and contractors; and reasonable security, when it takes effect in 2023. The CCPA also provides a private right of action for breaches of non-encrypted and non-redacted personal information. The CPA and VCDPA do not have a private right of action, for breach or any other violation of the law.

Processor Obligations

The CPA defines "processor" as the entity that processes personal data on behalf of a controller. Processors must:

- Follow the controller's instructions for processing;
- Assist the controller with responding to consumer requests; security — including breach notification; and risk assessments;
- Ensure confidentiality with respect to the data;
- Notify the controller of the use of any sub-processors, giving the controller the opportunity to object;
- Enter into a data processing agreement with the controller;
- Delete or return data to the controller at conclusion of the services;
- Demonstrate compliance and submit to audits by the controller or an auditor designated by the controller.

Again, these requirements largely track the VCDPA, except that the VCDPA does not require processors to give controllers the ability to object to a processor's engagement of a sub-processor. The CCPA imposes limitations on "service providers" and "third parties" and the CPRA will introduce limitations on "contractors" as well. These limitations focus on the use, sale, and disclosure of personal information outside of the business relationship between the business and the service provider or contractor.

Recommendations for Businesses

The increased focus on rights and accountability-based privacy regulation requires companies to assess their personal data handling practices and formalize their internal processes for handling such data.

First and foremost, businesses should gain a solid understanding of what personal data is collected, how and why it is used, where it is stored, how it is secured, and with whom it is shared and why. This "data mapping" or "data inventory" exercise will help an organization identify its internal personal data handling practices and determine what laws might apply.

Companies can then take a risk-based approach to managing that personal data. Are certain data stores more sensitive? Do certain processing activities pose greater risks to individuals? Are there specific laws coming down the pike that the company will need to comply with? Answering these questions will help the business determine the appropriate and necessary controls for managing personal data.

For transparency, the company should regularly review its privacy notice to confirm that it accurately describes what personal data is collected, how it is used, and with whom it is shared. Agreements with

vendors should be reviewed to ensure appropriate limitations and safeguards are in place. Records retention policies and schedules should be updated so that the company does not retain personal data for longer than necessary as keeping such data for too long poses significant risk. Lastly, to the extent consumer data rights will apply, the company should develop internal guidelines for receiving and classifying consumer requests, searching the appropriate repositories, and preparing a response.

As we head towards a patchwork of state regulation, companies will have to adopt internal processes that can be adapted to new laws or changing requirements. When viewed as a matter of “when” privacy rules will apply and not “if,” an organization can allocate the necessary resources to appropriately assess personal data handling practices and work to formalize policies and procedures that will help it achieve compliance in a timely way.