akerman

Practice Update

State Privacy Law Patchwork Expands as Colorado Passes Comprehensive Privacy Law

July 13, 2021

By Elizabeth F. Hodge, Christy S. Hawkins, and Kristen F. Morris

Colorado just became the third state to pass a comprehensive data privacy law, creating more challenges for businesses trying to navigate a variety of state, federal, and international privacy regimes. The Colorado Privacy Act ("CPA") will become effective July 1, 2023. Although the CPA includes many of the concepts in the California Consumer Privacy Act of 2018 ("CCPA"), the California Privacy Rights Act of 2020 ("CPRA"), and the Virginia Consumer Data Protection Act ("VCDPA"), how Colorado implements those concepts does not align perfectly with California or Virginia law, making it critical that organizations consider adopting a holistic approach to complying with their increasingly varied data privacy obligations.

Who Is Covered

The CPA applies to legal entities that conduct business in or deliver products and services that are intentionally targeted to Colorado residents, and meet one or both of the following thresholds: the entity either (1) controls or processes personal data of at least 100,000 Colorado residents annually, or (2) derives revenue or receives a discount on goods or services from selling personal data and processes or controls the personal data of at least 25,000

Related People

Christy S. Hawkins
Elizabeth F. Hodge
Kristen F. Morris

Related Work

Data Privacy and Security

Colorado residents. Unlike the CCPA and the CPRA, the CPA does not have a revenue threshold.

The new law applies to "personal data," which is information that is not publicly available and that is linked or reasonably linkable to an identified or identifiable individual. The CPA also recognizes "sensitive data," which is personal data that reveals racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status. Sensitive data also includes genetic or biometric data and personal data from a known child. As described below, the CPA imposes heightened requirements for the collection and processing of sensitive data.

Who Is Exempt From the CPA

Similar to the CCPA, CPRA, and VCDPA, the CPA does not apply to personal data that is already governed by certain federal and state privacy laws, such as protected health information, health-care information, and patient identifying information, and does not apply to certain entities. The exemptions are specific and can be complicated. For example, the CPA has data exemptions for information governed by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Gramm-Leach-Bliley Act, the Family Educational Rights and Privacy Act of 1974 ("FERPA"), and the Children's Online Privacy Protection Act of 1998 ("COPPA"). It also does not apply to certain activities regulated by the federal Fair Credit Reporting Act, such as those involving the collection, sale, or use of personal data that is related to creditworthiness or reputation when provided by a consumer reporting agency. Other exemptions include personal data maintained for employment records purposes, and customer data maintained by public utilities.

Notably, the CPA has entity exemptions for financial institutions and their affiliates that are subject to the Gramm-Leach-Bliley Act, national securities

associations registered pursuant to the Securities Exchange Act of 1934, and air carriers regulated under 49 U.S.C. § 40101, et. seq. and 49 U.S.C. § 41713. Finally, individuals acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context are excluded from the definition of a protected "consumer."

Key Provisions

Below is an overview of some of the notable provisions included in the CPA, including data subject rights, roles and responsibilities for controllers and processors, vendor and service provider relationships, privacy notice requirements, principles of data processing, and data protection assessments.

Controller and Processor Roles and Responsibilities. Like the VCDPA, the CPA designates businesses as controllers, i.e., an entity that determines the purposes for and means of processing personal data, and processors, i.e., an entity that processes personal data on behalf of a controller, and assigns rights and responsibilities to each. In general, a processor must follow the controller's instructions, protect the personal data entrusted to it, and assist the controller in meeting its obligations under the CPA.

Vendor and Service Provider Relationships. Similar to the CPRA and the VCDPA, the CPA requires that controllers and processors enter into a contract with specific requirements for processing and protecting personal data. This is not unlike the requirements set forth in Article 28 of the EU General Data Protection Regulation ("GDPR"), but the requirements under the CPA are not as extensive. Under the Colorado law, the contract must include processing instructions, details on processing, a promise to return or delete data after the contract is terminated, requirements to assist the controller in demonstrating compliance with the CPA, and a

requirement that the processor allows the controller to perform annual audits to ensure the processor is meeting its obligations under the contract.

Data Subject Rights. The CPA affords consumers similar privacy rights to those provided by the CPRA and the VCDPA, including the right of access, right to correction, right to deletion, and right to data portability. The CPA differs from the CCPA and CPRA in that it expands the right to opt out of sale of personal data by giving consumers the right to opt out of targeted advertising and profiling to make decisions that have significant effects on them. Additionally, the CPA requires that by July 1, 2024, a controller must allow consumers to use a universal opt-out mechanism to opt out. The Attorney General is responsible for establishing technical specifications for the opt-out mechanism.

Privacy Notice Requirements. Similar to its counterparts in California and Virginia, the CPA requires that controllers provide a privacy notice to consumers detailing the personal data practices for information collected by a controller or on its behalf. The notice must include the categories of personal data collected, the purposes for processing, how to exercise consumer privacy rights, and details of sharing and selling personal data with third parties.

Principles of Data Processing. The CPA requires that controllers follow certain principles and duties of data processing. These include the duty of purpose specification, data minimization, and limiting secondary use. Controllers have a duty of care to take reasonable security measures to secure personal data from unauthorized acquisition during storage and use. Controllers may not violate federal and state laws prohibiting unlawful discrimination against consumers when processing personal data. Finally, controllers must obtain the consumer's consent before processing sensitive data. These requirements are similar to the principles included in the VCDPA and CPRA.

Data Protection Assessments. In addition to imposing a duty on businesses to use reasonable security measures to protect personal data, the CPA also requires that the controller conduct data protection assessments for high-risk processing. The Act includes a list of circumstances that are considered high-risk, as well as the requirements that the data protection assessments must meet, including the benefits, risks, and mitigating safeguards of the intended processing.

Enforcement. The CPA gives enforcement authority exclusively to the Colorado state attorney general and district attorneys, and specifically states that it does not create a private right of action. Before taking legal action against a violator of the CPA, the attorney general or district attorney must issue a notice of violation to the controller, giving them sixty days to cure the violation. Violations of the CPA are deemed to be deceptive trade practices under the state's unfair or deceptive trade practices law.

Steps To Prepare For Compliance

While the CPA effective date is almost two years away, businesses should consider the following activities now:

1. Updating the organization's business privacy notice to ensure it conforms to the CPA's requirements;
2. Preparing processes and templates for conducting data protection assessments;
3. Auditing the business to ensure it has implemented the core principles for data processing into its operations;
4. Putting in place a process to respond to consumer privacy requests;
5. Begin the process of redrafting contracts with vendors as needed so that there are CPA-compliant contracts in place by the effective date; and

6. Ensuring that the business can demonstrate its compliance with the CPA requirements.

Businesses that start compliance efforts sooner rather than later and leverage their existing processes can ensure that compliance efforts are undertaken in a way that conserves resources and maximizes efficiency. In addition, given the other privacy laws that are pending and those that were proposed and failed this year, having a plan in place to achieve compliance can allow businesses to incorporate new requirements that arise as a result of additional state privacy legislation that may pass in the future.
