PUBLICATION

Another State Privacy Law Hits the Books: What You Need to Know About the Colorado Privacy Act

Authors: Matthew George White, Alexander Frank Koskey, III
July 08, 2021

Earlier this month, Colorado became the third state to pass comprehensive data privacy legislation. As we have previously analyzed, California originally passed the CCPA and the CPRA, then Virginia passed the VCDPA, and now Colorado has passed the Colorado Privacy Act (CPA). The CPA may be the newest piece of state comprehensive privacy legislation, but companies should continue to monitor developments in state laws as numerous other states continue to consider their own privacy legislation.

The CPA was signed into law by Colorado's Governor on July 7, 2021 and goes into effect on July 1, 2023. In many ways the CPA is similar to the CCPA and VCDPA; however, it does contain some important differences. This alert will examine several of the important provisions of the CPA and highlight several key areas where Colorado's legislation has new or different provisions than we have seen in California and Virginia.

Scope and Applicability

The CPA applies to entities that conduct business in Colorado or produce commercial products or services intentionally targeted to Colorado residents and (a) control or process personal data of at least 100,000 consumers per year; or (b) derive revenue or receive a discount on the price of goods or services from selling personal data or control personal data of at least 25,000 consumers. This threshold likely looks familiar, as it is substantially similar to the VCDPA; however, it removes the "50% of gross revenue" threshold contained in the VCDPA.

Also, like the VCDPA, the CPA defines a "consumer" as a Colorado resident acting in an individual or household context. The CPA does not include a person acting in a commercial or employment context, and therefore by definition excludes the personal data of employees or personal data collected from individuals in the context of business-to-business transactions, both of which have created significant questions as to their ultimate treatment under California's laws.

The CPA protects both "Personal Data" and "Sensitive Data." Personal Data is defined as "information that is linked or reasonably linkable to an identified or identifiable individual" and Sensitive Data is defined as Personal Data that reveals "racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual relationship, or citizenship or citizenship status" or "genetic or biometric data that may be processed for the purpose of uniquely identifying an individual" or personal data from a "known child" – an individual under 13 years of age.

Controllers and Processors

Like the VCDPA, the CPA incorporates the concepts of "Controllers" and "Processors." Under the Act, a Controller is a "person that, alone or jointly with others, determines the purposes for and means of processing personal data." A Processor is a "person that processes personal data on behalf of a Controller."

The CPA imposes varying obligations depending on whether the subject entity is a Controller or Processor. For a Controller, many of the duties mirror those seen in other privacy legislation, such as the EU's General Data

Protection Regulation (GDPR). These duties include, among others, (1) the duty of transparency; (2) the duty to obtain consent for processing sensitive data or children's data; (3) the duty of data minimization; (4) the duty of purpose specification; (5) the duty to avoid secondary uses; (6) the duty of care; (7) the duty to avoid unlawful discrimination; and (8) the duty to conduct data protection assessments. These duties will require that meaningful disclosures regarding an entity's privacy practices are clearly made in its privacy policies. Controllers will also need to establish processes for processing opt-out requests, appealing consumer rights decisions, and obtaining opt-in consent for processing of Sensitive Data or children's data and for conducting data protection assessments.

Processors will be required to enter into a data processing agreement with the Controller that defines the Processor's instructions, as well as specified obligations such as data retention and audit rights. Processors must also assist Controllers in responding to data subject requests, in conducting data protection assessments, and in meeting security and breach notification obligations. The CPA also requires that Processors maintain the confidentiality of any Personal Data they process, and that they provide Controllers with the opportunity to object to the use of any subcontractors (who in turn must also be engaged pursuant to a written agreement). Entities need to carefully assess any vendors they utilize to determine whether they would be Processors under the CPA, and if so, ensure the relationship complies with these requirements.

Consumer Rights and Compliance Obligations

The CPA borrows many of its consumer rights and compliance obligations from California and Virginia. These include:

- Giving consumers the right to opt out of the sale of personal data to third parties or the processing of personal data for targeted advertising, and

- Providing consumers with rights to (i) access personal data being processed by a controller; (ii) correct inaccuracies in their personal data; (iii) delete personal data provided by or obtained about the consumer; and (iv) data portability.

Broad Exemptions

The CPA contains several exemptions that are broader than other state privacy laws. Specifically, the CPA exempts personal data that is collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act (GLBA), as well as financial institutions or their affiliates that are subject to GLBA. This is a significant shift from other laws like the CCPA whose exemption only applied to data that is subject to the GLBA. The CPA also includes exemptions for covered entities and business associates under the Health Insurance Portability and Accountability Act (HIPAA), certain consumer reporting agencies and consumer reports, specified educational institutions, and de-identified data.

Rulemaking

The Colorado Attorney General has the authority to promulgate rules for the purpose of carrying out the CPA. One area in which the Attorney General has been required to issue rules relates to technical specifications for universal opt-out mechanisms. These must be published no later than July 1, 2023. Notably, unlike the CPRA which makes the global privacy controls optional, under the CPA Controllers must comply with the universal opt-out requirements. The CPA also explicitly provides that the Attorney General may adopt rules that govern the process of issuing opinion letters and interpretive guidance to develop an operational framework for businesses that includes a good faith reliance defense of an action that may otherwise constitute a violation of the CPA. If the Attorney General promulgates such rules, they must become effective by January 1, 2025.

Enforcement

The Colorado Attorney General and District Attorneys have exclusive authority to enforce violations of the Act. Penalties can be up to $20,000 for each violation, and each consumer involved can constitute a separate violation. The maximum penalty for a series of related violations is $500,000. The CPA also provides that a violation will be considered a deceptive trade practice. The Act does not contain a private right of action for consumers.

Key Takeaways

The CPA aggregates many terms, rights, and compliance obligations found in other privacy legislation like the GDPR, CCPA/CPRA, and the VCDPA. While there are some key differences that will need to be addressed, businesses that have worked toward compliance with these regulations should be able to leverage those efforts to comply with the CPA. However, if you have not yet developed a compliance framework for these other regulations, the CPA (as well as many other pending bills in other states) should provide a significant impetus for you to begin formulating a compliance plan. Covered entities should also monitor the Colorado Attorney General's forthcoming regulations to ensure compliance.

Compliance with these comprehensive privacy bills can require significant changes for many institutions. A good first step is to conduct a thorough data mapping exercise to determine what data you collect, where that data is stored, with whom you share that data, and when that data is deleted. Understanding your institution's data is a necessary first step toward developing your compliance program. We are happy to assist you in conducting a data mapping exercise, in interpreting the results, and in using that information to develop a program to comply with the CPA or any other state privacy legislation.

If you have any questions regarding the CPA, other state privacy legislation, or any other aspect of your privacy management program, please contact the authors, Matthew G. White, CIPP/US, CIPP/E, CIPM, PCIP, or Alexander F. Koskey, CIPP/US, CIPP/E, PCIP, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.