Cooley

Colorado Becomes Third State to Pass a Comprehensive Privacy Law

July 8, 2021

On July 7, 2021, Colorado Gov. Jared Polis signed the Colorado Privacy Act (CPA) into law. The CPA is now the third comprehensive consumer privacy law to be passed in the United States, after the California Consumer Privacy Act (CCPA) and Virginia's Consumer Data Privacy Act (CDPA). Enforcement of the CPA will begin July 1, 2023.

While the CPA is similar to the CCPA and CDPA, certain elements distinguish the Colorado law from its counterparts and will require additional compliance efforts from companies that fall within its jurisdiction.

Who does the CPA apply to?

The CPA applies to legal entities that conduct business or produce products or services that are intentionally targeted to Colorado residents and that (i) control or process data from at least 100,000 consumers (as defined below), or (ii) control or process data from at least 25,000 consumers and also derive some portion of their revenue or receive a discount on the sale of goods or services from the sale of personal data. The definition of a "consumer" under the CPA is notably narrower than the CCPA, and only includes a Colorado resident acting in an individual or household context.

The CPA exempts data being processed in a commercial or employment context, such as information from a job applicant, but there is ambiguity as to whether this business-representative exclusion equals that of the CCPA. "Controllers" or "processors" (as defined below) are not restricted in their ability to use data for internal research purposes to improve, repair, or develop products, services or technology.

The CPA also does not apply to data subject to certain federal privacy regulations, including the Gramm-Leach-Bliley Act, the Driver's Privacy Protection Act of 1994, the Children's Online Privacy Protection Act of 1998, the Family Educational Rights and Privacy Act of 1974, and the Health Insurance Portability and Accountability Act. It likewise exempts data maintained for employment records or noncommercial purposes by certain public utilities, state institutions of higher education and judicial departments.

What information does the CPA cover and what rights does it give to consumers?

The CPA applies to the controlling or processing of "personal data," which is defined broadly as information that's linked or reasonably linkable to an identified or identifiable individual. As drafted, the law is ambiguous as to what information may be treated as "reasonably linkable" under this definition. Like the CCPA and CDPA, personal data does not include de-identified data or "publicly available" information, which refers to data lawfully made available from government records or that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public.

Consistent with other privacy laws, the CPA affords consumers certain rights, which can be exercised by a consumer up to two times per calendar year per company:

- Access to confirm whether a controller is processing personal data
- Correction of any inaccuracies in the personal data collected
- Deletion of any consumer-related information
- Portability of data so it can be transmitted from one entity to another in a readily usable format

In a significant deviation from the other privacy laws, the CPA also allows consumers to opt out of the sale, collection and use of personal data in certain circumstances. In particular, a consumer has the right to opt out of the processing of personal data for purposes of profiling, in addition to opting out of targeted advertising and the "sale" of personal data. Activities that constitute a sale are also arguably narrower under the CPA, specifically requiring an exchange of personal data for monetary or other valuable consideration by a controller to a third party.

When enforcement begins on July 1, 2023, controllers engaged in targeted ads or the sale of personal data must have a clear and conspicuous way for consumers to opt-out of collection. By 2024, this individualized format will be phased out and replaced by a universal opt-out mechanism, which the Attorney General's office is tasked with creating and deploying. This makes the CPA the first privacy law to require companies to employ universal opt-out technologies.

What does the CPA require from businesses?

The CPA defines a data controller similarly to the CDPA as an entity that, alone or jointly with others, determines the purpose and means of processing personal data. Also consistent with the CDPA's definition, a processor is an entity that processes personal data on behalf of a controller. A third party is a person, public authority, agency or other body – other than a consumer, controller, processor, or affiliate of the processor or controller.

To protect personal data, the CPA requires controllers and processors to do all of the following:

- Give consumers a privacy notice that is reasonably accessible, clear and meaningful
- Specify the express purposes for which they are collecting and processing personal data
- Make sure that the collection of personal data is adequate, relevant and limited to what is reasonably necessary in relation to those specified purposes (avoiding secondary use)
- Refrain from processing personal data for purposes that are not reasonably necessary for the specified purposes without a consumer's consent
- Take reasonable measures to secure personal data from unauthorized acquisition during storage and use
- Avoid unlawful discrimination
- Provide opt-in consent for the processing of "sensitive data," which is defined as data that reveals information about race, gender, ethnicity, religious beliefs, sexuality or citizenship, as well as genetic or biometric data

Similar to the CDPA, a controller must complete data protection assessments if they are engaged in processing personal data that presents a "heightened risk of harm to consumers," such as (i) processing personal data for targeted advertising or profiling (if profiling presents a reasonably foreseeable risk of substantial injury to consumers), (ii) selling personal data, or (iii) processing sensitive data. An assessment must identify and weigh the benefits that might flow from the processing of personal data against the potential risks to the rights of the consumer, and the results of the assessment must be made available to the State Attorney General upon request.

With relation to consent, the CPA diverges from the CCPA and CDPA by explicitly rendering illegitimate any consent obtained through the use of "**dark patterns**," which are defined as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice." Dark patterns have recently been subject to increasing

legislative scrutiny, as they are often used to coercively influence user behavior, such as making it difficult to find where to unsubscribe or opt out of the sale of personal information.

Processors must help the controller meet its obligations related to the security of processing personal data and notify the controller in the event of a security breach. Additionally, processors are subject to a duty of confidentiality, implementing reasonable security and training protocols to safeguard personal data.

How is the CPA enforced?

The CPA explicitly states that it offers no private right of action to consumers. Enforcement powers belong solely to the Colorado Attorney General or District Attorneys. In the event of noncompliance, the attorney general or district attorneys must issue a notice of violation to a controller if a cure of the noncompliant behavior is deemed possible. If the controller fails to cure within 60 days, or if a cure is not deemed possible, the attorney general or district attorney can bring an enforcement action. A violation of the CPA would be classified as a deceptive trade practice and could result in a $20,000 fine per violation, with no cap on the total fine imposed.

What do clients and businesses need to do to comply with the CPA?

While clearly modeled after the CCPA and CDPA, the CPA has a few key provisions that companies may need to pay special attention to by July 1, 2023.

First, the CPA has geographically targeted applicability to activities aimed at Colorado residents, rather than a monetary threshold. Each company will need mechanisms to monitor how many Colorado residents or households have provided personal data to the company.

Companies will need to implement a means for consumers to opt out of the processing of their personal data for purposes of profiling, and will need to avoid the use of dark patterns for obtaining opt-in consent from consumers. Moreover, by 2024, companies will need systems in place to respond to reasonable universal opt-out requests via browser controls or other mechanisms.

Due to the CPA's limitations on secondary use, companies should strive to ensure that their privacy policies clearly and adequately list all current and foreseeable purposes for personal data collection, or otherwise obtain opt-in consent for additional purposes. Finally, many companies will need to annually prepare data protection assessments that weigh the benefits of their data collection purposes against the risks to consumers.

Key Contacts

Andrew Epstein Seattle	aepstein@cooley.com +1 206 452 8747