DAVIS GILBERT

Digital Media, Technology + Privacy

Colorado Privacy Act Becomes the Third Comprehensive State Privacy Law

The Bottom Line

- Colorado is the third state to enact a comprehensive consumer privacy law.
- Although the Colorado Privacy Act shares some similarities with California's CCPA and CPRA, and Virginia's CDPA, there are some material differences, and companies will need to strategize how to harmonize their privacy programs with the various state privacy laws coming into effect.

After passing through the Colorado General Assembly, Governor Jared Polis signed the Colorado Privacy Act (CPA) into law on July 7, 2021. Colorado is now the third state in the country – following California and Virginia – to pass comprehensive privacy legislation. Companies that are subject to the CPA will have to comply beginning July 1, 2023, the date when the new law goes into effect.

Details of the CPA

The CPA adopts the "controller-processor" framework found in the European General Data Protection Regulation (GDPR). The bulk of the CPA's obligations will apply to controllers that conduct business in Colorado or produce products or services that are targeted to Colorado residents, and that control or process the personal data of at least:

- 100,000 "consumers" during a calendar year; or
- 25,000 "consumers," and derive revenue or receive a discount on the price of goods or services from the "sale" of personal data.

A notable difference between the CPA and its California and Virginia counterparts is that there is no revenue threshold for applying the law. For companies that control or process the data of at least 25,000 consumers, it is sufficient that they derive ***any*** revenue or receive ***any*** discount on goods or services in return for selling personal data. As such, companies that are not subject to the California Consumer

Privacy Act (CCPA), California Privacy Rights Act (CPRA), or the Virginia Consumer Data Protection Act (CDPA) because of those laws' revenue requirements may still be subject to the Colorado law.

Consumer

The term "consumer" only includes Colorado residents that are acting in an individual or household context and specifically excludes persons acting in a commercial or employment context. Accordingly, businesses do not need to consider data collected from their employees or from business contacts as personal data under the CPA.

Sale of Personal Data

The "sale" of personal data is defined as "the exchange of personal data for monetary consideration or other valuable consideration by a controller to a third party." Because the definition includes "other valuable consideration" as well as "monetary consideration," the exchange of personal information (such as cookie data) for targeting and serving advertising to users across different platforms might qualify as a sale. This definition closely resembles the current CCPA definition of sale, and is broader than the forthcoming CDPA, which limits sales to exchanges for monetary consideration. The CPA also provides several exceptions to the definition of sale.

Duties For Controllers

The Colorado law outlines specific duties that controllers must follow:

Transparency: Controllers must provide consumers with a "reasonably accessible, clear, and meaningful privacy notice."

Purpose specification: Controllers must "specify the express purposes for which personal data are collected and processed."

Data minimization: Collection of personal data must be limited to what is reasonably necessary for the specified purposes for data processing.

Avoid secondary use: Controllers cannot process personal data for reasons that are incompatible with the specified processing purposes without a consumer's consent.

Duty of care: Controllers must implement reasonable measures to safeguard personal data from unauthorized acquisition.

Avoid unlawful discrimination: Controllers must not process data in violation of federal and state anti-discrimination laws.

Consumer Rights

The CPA provides a series of rights, similar to those found in the CDPA, which may be exercised pursuant to statutorily-sanctioned methods. In particular, the CPA grants rights to consumers:

- To confirm whether or not a controller is processing their personal data, and the ability to access such data;
- To correct inaccuracies in their personal data;
- To delete their personal data;
- To obtain a copy of personal data that they have provided to the controller in a portable and, to the extent technically feasible, readily usable format; and
- To opt-out of certain types of processing, including the sale of personal data, the use of personal data for purposes of "targeted advertising," and "profiling" that produces legal or similarly significant effects for the consumer. Importantly, the CPA allows consumers to authorize another person, acting on their behalf, to perform the opt-out. This includes the use of technology that indicates a consumer's intent to opt out, including web links, browser extensions, and global device settings.

Data Protection Assessments

Similar to the CDPA, the CPA requires companies to conduct and document a "data protection assessment" of activities that present "a heightened risk of harm to a consumer," identifying and weighing the benefits of the processing activity against the potential risks to consumer rights. Activities requiring a data protection assessment include:

- Sales of personal data;
- Processing personal data for targeted advertising;
- Profiling that presents certain risks to the consumer; and
- Processing sensitive data.

Unlike the CPRA's similar rule for businesses to submit mandatory "risk assessments" to California regulators on a "regular basis," the CPA only requires that companies make data protection assessments available to the Colorado Attorney General upon request.

Sensitive Data

The CPA's definition for "sensitive data" tracks closely with the CDPA. Importantly, unlike the CPRA and CDPA, the CPA does not treat "precise geolocation" as a form of sensitive data or provide any definition for that term.

The CPA requires controllers to obtain a consumer's opt-in consent to process sensitive data. Additionally, the CPA expressly provides that processing sensitive data is an activity that creates "a heightened risk of harm" to consumers, warranting a data protection assessment.

Dark Patterns

The CPA expressly provides that an individual's consent is invalid if obtained through "dark patterns," defined as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice." Similar treatment of dark patterns can also be found in the forthcoming CPRA, but not the CCPA. The law's emphasis on dark patterns reflects a growing concern over practices such as designing privacy settings in a purposely confusing way or creating hidden stipulations that are difficult for the average user to understand.

Universal Opt-Out

By July 1, 2023, the Colorado Attorney General is required to adopt rules detailing specifications for "universal opt-out mechanisms" that will allow consumers to exercise their choice to opt out of processing for targeted advertising or sales. Possibly anticipating the complications that could arise from multiple state laws requiring their own "Do Not Sell" links or equivalent mechanisms, the CPA requires the Attorney General to "[a]dopt a mechanism that is as consistent as possible with any other similar mechanisms required by law or regulation in the United States."

Enforcement

The CPA is enforceable solely by the Colorado Attorney General and local district attorneys. The law explicitly states that it does not create a private right of action. Unlike the forthcoming CPRA and CDPA, which function independently from their respective states' consumer protection laws, violations of the CPA constitute a *per se* "deceptive trade practice" under the existing Colorado Consumer Protection Act. The Attorney General or district attorneys can seek injunctive relief or civil penalties of up to $20,000 per violation. Each consumer or transaction involved constitutes a separate violation.

For the time being, the Attorney General or local district attorney must issue companies a notice of violation and grant them 60 days to cure such violation before bringing an enforcement action. However, this notice and cure provision expires January 1, 2025.

For More Information

Please contact the attorneys listed below or the Davis+Gilbert attorney with whom you have regular contact.

Gary A. Kibel

Partner
212 468 4918
gkibel@dglaw.com

Zachary N. Klein

Associate
212 237 1495
zklein@dglaw.com