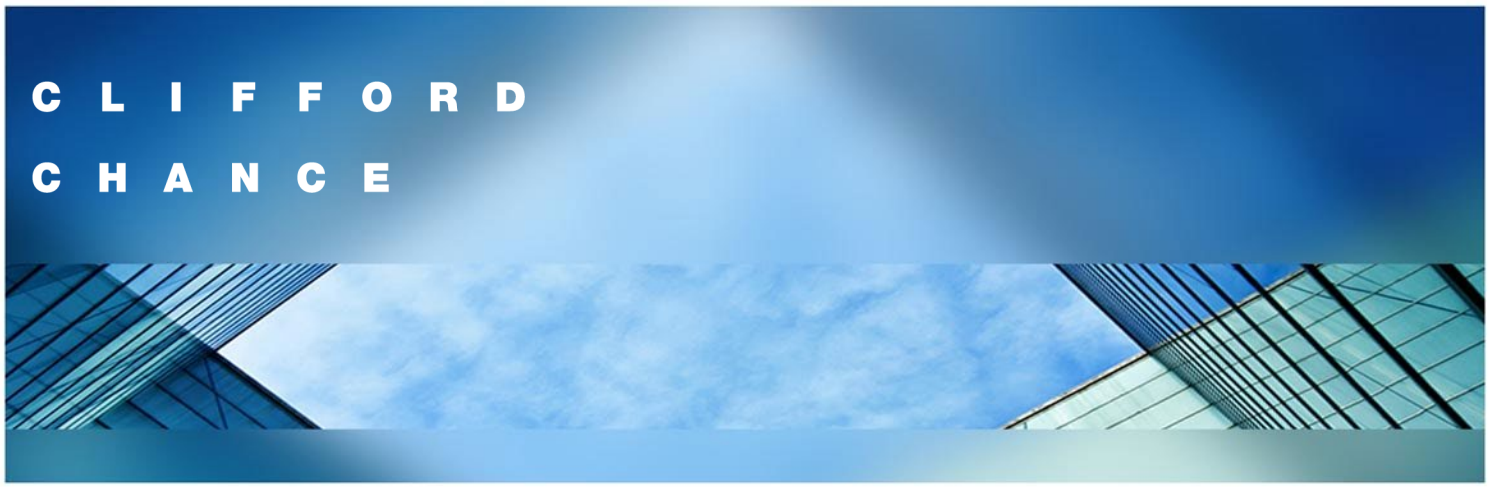

COLORADO JOINS CALIFORNIA AND VIRGINIA WITH A COMPREHENSIVE DATA PRIVACY LAW

On July 8, 2021, Colorado Governor Jared Polis signed the Colorado Privacy Act (CPA), making his state the third to enact a comprehensive consumer privacy law. Although there are some key differences, the CPA largely parallels both the California Privacy Rights Act (CPRA)[1] and the Virginia Consumer Data Protection Act (VCDPA), and will give Colorado consumers certain rights with respect to their personal data. The new law will go into effect on July 1, 2023.

Key issues

- Colorado became the third state to enact a comprehensive consumer privacy law.
- The statute is largely aligned with similar laws in California and Virginia, but there are key differences companies should keep in mind as they update their compliance measures.
- The Colorado Attorney General and state district attorneys can enforce the statute. However, companies can take solace that for the first 18 months after the law goes into effect, they will have a 60-day cure period following notice of an alleged violation.
- The law does not provide for a private right of action.

OVERVIEW OF THE CPA

Scope: Which Entities Must Comply

The CPA only applies to "controllers"[2] that have a significant presence or business interest in the state—specifically, controllers that either:

- Conduct business in Colorado; or
- Produce or deliver commercial products or services that are intentionally targeted to Colorado residents.

This requirement closely mirrors the nexus requirement of the Virginia statute and goes beyond that of the California law (which only applies to controllers that "do business" in the state). Unfortunately, none of the statutes so far have defined what it means to conduct business in their respective states, leaving some uncertainty for companies considering whether they are in scope of these laws.

Additionally, the statute specifies that it applies only to a controller that satisfies one of two thresholds:

- It controls or processes the personal data of 100,000 Colorado residents per calendar year; or

[1] The CPRA amends and adds to the California Consumer Privacy Act (CCPA), the data privacy law currently in effect in California. The CPRA goes into effect on January 1, 2023. Unless specified, this briefing compares the Colorado law with the CPRA.

[2] The statute defines "controller" to mean any entity that, alone or jointly with others, determines the purposes for and means of processing personal data.

- It controls or processes the personal data of at least 25,000 Colorado residents per calendar year and derives revenue from the sale of personal data.

Interestingly, the second threshold only requires that a controller derive any revenue from the sale of personal data, including if the controller receives a discount on goods or services in exchange for personal data. This is broader than the revenue requirements under the California and Virginia statutes, both of which specify that they apply only to certain entities that derive *over half* of their gross revenue from the sale of personal data.

Despite being slightly broader in scope than California's and Virginia's state laws, these requirements nevertheless will mean that many small businesses will be exempt from the requirements of the Colorado law.

Exemptions: What Data is Not Covered

The CPA carves out from its protections personal data that is already protected by other laws and regulations, such as the Gramm-Leach-Bliley Act (*i.e.* personal data collected by financial institutions) and the Health Insurance Portability and Accountability Act (*i.e.* personal information collected by health institutions). The law also defines "consumer" to exclude individuals acting in a commercial (*i.e.* representing a business) or employment context, meaning data collected in those contexts will not be covered by the law.

Additionally, the CPA makes clear that its provisions are not meant to prevent controllers from fulfilling other obligations, such as complying with other laws, responding to a subpoena or similar government inquiry, cooperating with law enforcement, exercising or defending legal claims, performing a contract, maintaining legal privilege, or exercising free speech. Similarly, controllers can use personal data notwithstanding the CPA's restrictions for internal functions such as research and development, cybersecurity, and fraud prevention.

These exemptions are similar to those that appear in the Virginia law. The California law also contains certain exemptions for personal data covered under other statutory regimes (*e.g.* the Gramm-Leach-Bliley Act). However, it is not yet clear how the law will apply to information collected in a commercial or employment context—the current law (the CCPA) exempts this data, but these exemptions are due to sunset on January 1, 2023, when the CPRA goes into effect. It will be interesting to see how the legislature will treat this data—or if it joins Virginia and Colorado in carving it out entirely.

Consumer Rights

The CPA establishes five main consumer personal data rights:

- the right to **opt out** of certain processing, including for the purposes of targeted advertising, sale of personal data, or profiling with a legal or significant effect;
- the right to **access** collected data (including the right to confirm whether a controller is processing the consumer's personal data)
- the right to **correct inaccuracies** in the consumer's personal data;

- the right to **deletion** of the consumer's personal data;
- the right to **data portability** (*i.e.* request personal data in a format that can be transmitted to another party).

The statute also provides some protections for consumers to ensure that these rights can be exercised freely. First, opt-out mechanisms must be "clear and conspicuous." And where consent is required, it must involve a "clear, affirmative act" and be "freely given, specific, informed, and unambiguous." Specifically, consent cannot be obtained through general or blanket consent terms, implied from certain interaction with content (hovering over, muting, pausing, or closing a piece of content), or agreements obtained through dark patterns (designs meant to manipulate users). The statute also requires controllers to allow consumers to exercise opt-out rights through browser signals as well as a universal opt-out mechanism to be developed by the Attorney General.

These rights and protections parallel those provided in the California and Virginia statutes with minor differences, including using the California law's slightly broader definition of "sale"[3] and specifying how controllers should provide opt-out rights (like California and unlike Virginia).

Notice Requirements

The CPA imposes a "duty of transparency" on controllers, requiring them to provide consumers with a "reasonably accessible, clear, and meaningful privacy notice," which includes information on:

- categories of personal data that are processed;
- the specific purposes for processing, including sales or use for targeted advertising;
- how consumers can exercise their rights, including opting out of sales or targeted advertising.
- what categories of personal data are shared with third parties (if any); and
- what categories of third parties (if any) to which personal data is shared.

These notice requirements closely align with those of the California and Virginia laws, although the California law has gone further to require some additional reporting for certain entities significantly involved in consumer data processing (*i.e.* buying, receiving, selling, or sharing the personal information of at least 10 million California consumers).[4]

Duties of Controllers

The CPA imposes a number of "duties" on controllers, including:

- **minimization**—only collecting consumer data that is "adequate, relevant, and reasonably necessary" for the purposes disclosed to the consumer;

[3] Virginia defines a "sale" of personal data to mean the exchange of personal data for monetary consideration. The California and Colorado statutes define "sale" to also include "other valuable consideration."

[4] This requirement is part of the law's implementing regulations, § 999.317(g).

- **avoidance of secondary use**—not processing personal data for purposes that are not reasonably necessary or compatible with specified purposes, absent consent;
- **care**—taking reasonable measures to secure personal data during storage and use, appropriate to the volume, scope, and nature of the personal data and the business;
- **non-discrimination**—not processing data in a manner that violates state or federal anti-discrimination laws; and
- **sensitive data protections**—obtaining consent before processing sensitive data such as race or ethnic origin, religious beliefs, mental or physical health conditions or diagnoses, sex life or sexual orientation, citizenship or citizenship status, biometric or genetic data (used to identify an individual), or children's data.

The CPA also prohibits controllers from increasing the cost of or decreasing the availability of a product or service as a result of a consumer's decision to exercise one of these rights, unless the product or service is related to a consumer's personal data (*e.g.* a voluntary loyalty or discount program).

These rights closely match those found in the Virginia law. Similar principles can be found in the California law, although they are formulated slightly differently—for example, there is no specific duty of minimization, but California law requires that a business's data processing is "reasonably necessary and proportionate," which could be read to imply such a duty.

Interestingly, there are some minor differences regarding how Colorado defines "sensitive" personal information compared to its sister states. Colorado's definition matches Virginia's definition almost word for word, but excludes precise geolocation, an interesting omission given some of the ongoing investigations and litigation against Big Tech companies like Google over this type of data collection. This also means Colorado's definition of "sensitive" personal information is significantly more limited than California's definition, which includes social security numbers and government IDs, financial account information, union membership, and the contents of a consumer's communications that are not directed towards the controller.

Additionally, Colorado (like Virginia) only briefly mentions children's data, choosing to include in its definition of sensitive information personal data collected from individuals under age 13.[5] California, on the other hand, provides a host of specific and tiered protections and policies that a controller must have in place for data collected from consumers under age 13 and between the ages of 13 and 16.

Data Protection Assessments

Controllers also have the "duty" to conduct a data protection assessment on any processing that presents a "heightened risk" of harm to a consumer. This includes:

- processing personal data for **targeted advertising**;

[5] The statute also completely exempts data regulated under the Children's Online Privacy Protection Act (COPPA).

- **profiling**, where there is a reasonably foreseeable risk of financial or physical injury or other substantial injuries to the consumer;
- **selling** personal data; and
- processing **sensitive data**.

These assessments require controllers to balance the risks and benefits of the processing to the controller, the consumer, other stakeholders, and the public in considering whether and how to proceed with this type of processing. The CPA also requires controllers to consider what safeguards can be put in place to reduce risks, as well as reasonable expectations of the data subject and the context of the processing. The results of these assessments must be documented and available to the Colorado Attorney General on request.

Virginia has almost identical data protection assessment requirements. California, on the other hand, has left it to regulators to prescribe so-called "risk assessments," although the statute does direct regulators to issue regulations that require entities to conduct risk assessments for processing that presents a "significant risk" to consumer privacy or security, so in practice all three states will likely have similar requirements.

Processors

The new Colorado law also imposes certain obligations on vendors (or "processors"), including:

- Adhering to the instructions of the controller providing the data;
- Assisting the controller in complying with the statute;
- Implementing appropriate technical and organizational measures to protect the security of the personal data;
- Helping controllers protect the security of personal data, and assisting with breach notification when necessary;
- Assisting controllers in responding to consumer rights requests;
- Providing controllers with notice and an opportunity to object before engaging subcontractors; and
- Providing controllers with information necessary to perform data protection assessments.

Processors must also permit controllers to audit compliance with these requirements.

Controllers must put in place contracts with processors that set out these requirements. The contracts must also provide processing instructions, explain the type of data subject to the processing and the duration of that processing, and require processors to delete or return personal data once the services conclude.

This provisions are almost identical to the requirements in Virginia, and both go beyond California, which requires entities to impose on certain third parties contractual requirements that (1) limit the purposes for which data can be shared;

(2) comply with applicable statutory requirements; and (3) prohibit selling or disclosing personal information for purposes not set out in the contract.

Penalties & Enforcement

The Colorado Attorney General has authority to enforce the CPA, including seeking injunctive relief and civil penalties. The statutes establishes that a violation is a deceptive trade practice, incorporating Colorado consumer protection laws, which provide for a range of penalties up to $20,000 per violation.

Notably, the law provides for a 60-day cure period before the government is permitted to pursue an enforcement action. This notice-and-cure provision is only temporary, however, sunsetting on January 1, 2025.

The law explicitly excludes a private right of action, specifying that only the Colorado Attorney General and state district attorneys will have authority to enforce the law.

This enforcement scheme is similar to those provided under the California and Virginia statutes, with differences in the specifics. For example, while Colorado mandates a 60-day cure period during the law's first 18 months, Virginia's cure period requirement is permanent, but only 30 days, whereas California gives regulators discretion to provide a cure period. The California also goes further in providing regulators with enforcement tools, establishing a state agency focused solely on data protection (the California Privacy Protection Agency).

Summary of Key Differences

As this analysis has shown, while the Colorado statute is closely aligned with both the data privacy laws in California and Virginia, there are some key differences companies should note when preparing for compliance, including:

- Having a slightly broader scope of application than either of its sister states;
- Following Virginia in permanently exempting personal data collected in the employment and commercial context;
- Specifying certain mechanisms for opt-out that businesses must accept;
- Having the most limited definition of what information is considered to be "sensitive" (and thus subject to heightened protections);
- Following Virginia in requiring data protection assessments for high-risk data processing; and
- Following Virginia in imposing requirements on processors (both directly and through required contractual restrictions from controllers).

Companies should also be aware of the nuances in the state's enforcement regime that differ from California's and Virginia's.

CONCLUSION

Colorado is the latest state to enact comprehensive privacy legislation, but it would not be surprising for that to change soon. As the nation moves back to business as usual, legislators will increasingly turn their attention to issues like

data protection, especially given the recent media focus on Big Tech and privacy. And as more states enact privacy laws, other states will feel pressure to not be left behind, potentially creating a snowball effect. This in turn will increase pressure on federal lawmakers to pass national data protection legislation, support for which has steadily been growing in recent years.

In any case, this means companies—especially those that do business in multiple states—must ensure that they continually review their data protection and privacy policies to maintain compliance with this shifting patchwork of US laws. Fortunately, Colorado lawmakers chose to align their statute closely with those of California and Virginia. Nevertheless, there are still some key differences among the statutes, so companies that are potentially in scope of the new Colorado law should begin considering now what changes they need to make to be compliant with the law once its requirements kick in on July 1, 2023.

CONTACTS

Celeste Koeleveld
Partner

T +1 212 878 3051
E celeste.koeleveld
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Philip Angeloff
Counsel

T +1 202 912 5111
E philip.angeloff
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA