THOMSON REUTERS
PRACTICAL LAW™

Preparing for Compliance with the Colorado Privacy Act Rules

by Rachel Marmor, Holland & Knight, with Practical Law Data Privacy & Cybersecurity

Status: **Published on 16 Jun 2023** | Jurisdiction: **Colorado**

This document is published by Practical Law and can be found at: **content.next.westlaw.com/w-039-2435**
Request a free trial and demonstration at: **tr.com/practicallaw-home**

An Article discussing the Colorado Privacy Act (CPA) Rules' unique requirements that create additional compliance steps for businesses. This Article details the history of the CPA and its Rules, the CPA's main requirements, and the new obligations the CPA Rules create around privacy notice details, data protection impact assessments, processing restrictions, sensitive data, and honoring universal opt-out signals. This Article also discusses steps businesses can take to best position themselves for compliance ahead of the July 1, 2023 CPA effective date.

The US state consumer privacy landscape is in a period of rapid development. Colorado became the third state, following California and Virginia, to provide consumers with comprehensive privacy protections when it enacted the Colorado Privacy Act (CPA) (Colo. Rev. Stat. Ann. §§ 6-1-1301 to 6-1-1313). Since then, several other states have passed consumer privacy laws, including Utah, Connecticut, Iowa, Indiana, and Tennessee, and many other states have bills in the legislative process. While complying with multiple states' laws already presents a challenge for businesses, the Colorado Attorney General's (CO AG) office has used its rulemaking power to add complexity to the CPA, creating an additional burden on businesses operating in Colorado as they prepare for the July 1, 2023 effective date.

This Article provides a history of the CPA and its rulemaking process, gives an overview of the law, discusses some of the CPA Rules' unique requirements, and provides recommendations on how businesses can best prepare for and achieve compliance.

For more information on other state privacy laws, see State Data Privacy Laws Toolkit and State Consumer Privacy Legislation Tracker.

For interactive and customizable charts that compare the CPA's requirements to other state consumer privacy laws, see Quick Compare Charts:

- State Consumer Privacy Laws – Overview.
- State Consumer Privacy Laws – Consumer Rights.
- State Consumer Privacy Laws – Excluded Entities or Data.
- State Consumer Privacy Laws – Statutory Use Exceptions.

History of the CPA

The CPA was enacted on July 7, 2021 and takes effect on July 1, 2023. At the time of enactment, the obligations of the law looked very similar to those of Virginia's law (Va. Code Ann. §§ 59.1-575 to 59.1-584; see Practice Notes, Colorado Privacy Act (CPA) Quick Facts: Overview and Virginia Consumer Data Protection Act (VCDPA) Quick Facts: Overview). However, the CPA granted the CO AG authority to make rules to facilitate its enforcement. The CPA Rules, which the CO AG filed on March 15, 2023, contain 44 pages of specific requirements on how a business must comply with the CPA, adding new areas of emphasis and making the compliance burden significantly more complicated in Colorado than in Virginia and other states (4 Colo. Code Regs. §§ 904-3:1.01 to 904-3:11.02). The Rules also take effect on July 1, 2023. For a history of the CPA rulemaking process, see Practice Note, Colorado Privacy Act Regulation Tracker.

CPA Law Overview

Definitions and Scope

The CPA:

- Defines consumers as Colorado residents acting in an individual or household context, which excludes workforce members and business-to-business contacts (Colo. Rev. Stat. § 6-1-1303(6)).
- Defines personal data broadly as information that is linked or reasonably linkable to an identified or identifiable individual (Colo. Rev. Stat. § 6-1-1303(17)).

- Defines sensitive data to include:
  - personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status;
  - genetic or biometric data that may be processed to uniquely identify an individual; or
  - personal data from a known child.

  (Colo. Rev. Stat. Ann. § 6-1-1303(24).)
- Applies to entities that conduct business in Colorado and either:
  - control or process the personal data of 100,000 or more consumers in a calendar year; or
  - sell personal data to derive revenue or receive a discount on goods or services, and control or process the personal data of 25,000 or more consumers.

  (Colo. Rev. Stat. Ann. § 6-1-1304(1).)
- Contains broad exceptions where specific types of information are already covered by law, for example:
  - health information protected under the Health Insurance Portability and Accountability Act of 1996;
  - financial information regulated by the Gramm-Leach-Bliley Act;
  - information from motor vehicle departments regulated under the federal Driver's Privacy Protection Act of 1994;
  - information regulated by the Children's Online Privacy Protection Act of 1998 (COPPA); and
  - information used in activities subject to the Fair Credit Reporting Act.

  (Colo. Rev. Stat. Ann. § 6-1-1304(2).)

Colorado is the only state that does **not** exclude non-profit organizations from the definition of an in-scope business. Colorado exempts financial institutions subject to GLBA in their entirety but also goes further than Virginia, for example, by including certain entities in the full exemption list such as air carriers, national securities associations, and public utilities. (Colo. Rev. Stat. Ann. § 6-1-1304(2)(j)(III)-(IV), (l), (n).) For more on the CPA's data and entity exceptions, see Practice Note, Colorado Privacy Act (CPA) Quick Facts: Overview: Excluded Entities or Data.

Controller Obligations

The CPA's controller duties and obligations include:

- Transparency (privacy notice).
- Purpose specification and limitation.
- Data minimization.
- To avoid secondary use.
- Care (security).
- To avoid unlawful discrimination.
- To obtain consent before processing sensitive data.

(Colo. Rev. Stat. Ann. § 6-1-1308; see Restrictions on Data Use.)

The CPA also requires controllers to act on and respond to a consumer's request to exercise their personal data rights to:

- Access.
- Correction.
- Deletion.
- Data portability.
- Opt out of:
  - personal data sales;
  - targeted advertising; or
  - profiling for decisions producing legal or similarly significant effects.

(Colo. Rev. Stat. Ann. § 6-1-1306; see Consumer Rights.)

Controllers must also conduct data protection assessments (DPIAs) before engaging in personal data processing activities that present a heightened risk of consumer harm, for example:

- Targeted advertising.
- Selling personal data.
- Processing sensitive data.
- Profiling that presents a reasonably foreseeable risk of:
  - unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
  - financial or physical injury to consumers;
  - a physical or other intrusion on consumers' solitude, seclusion, private affairs, or private concerns, if it would offend a reasonable person; or
  - other substantial consumer injury.

(Colo. Rev. Stat. Ann. § 6-1-1309; see Data Protection Impact Assessments.)

Processor Obligations

The CPA requires processors to:

- Adhere to the controller's instructions.
- Help the controller meet its obligations, considering the nature of processing and available information, including the controller's obligations to:
  - respond to consumer rights requests;
  - comply with data security and breach notification requirements; and
  - conduct data protection assessments.
- Ensure each person processing personal data is under a duty of confidentiality.
- Only engage subcontractors after:
  - giving the controller a chance to object; and
  - executing a written contract requiring the subcontractor to meet the same personal data obligations as the processor.
- Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, considering the processing context and the processor's role.
- Execute written processing agreements with specific terms.

(Colo. Rev. Stat. Ann. § 6-1-1305.)

Rulemaking and Enforcement Authority

The CPA grants the CO AG rulemaking and enforcement authority and specifically states that CPA violations do not form a basis for a private right of action (Colo. Rev. Stat. Ann. §§ 6-1-1310, 6-1-1311, and 6-1-1313). Colorado law considers violations of the CPA an unfair trade practice and imposes fines of up to $20,000 per violation or up to $50,000 per violation when the individual harmed is an elderly person (Colo. Rev. Stat. Ann. § 6-1-112(1)(a), (c)).

The CPA Rules' New and Unique Requirements

Businesses that took steps to comply with California and Virginia's laws ahead of January 1, 2023 may find that they have the building blocks in place for CPA compliance. However, they must closely review the CPA Rules for new, different, or more detailed compliance obligations, for example, those on:

- Offering and honoring consumer rights (see Consumer Rights).
- Implementing data processing restrictions (see Restrictions on Data Use).
- Conducting data protection impact assessments (see Data Protection Impact Assessments).

Consumer Rights

Like most state consumer privacy laws, the CPA grants consumers the right to access, delete, and correct their personal data and the right to data portability. It also gives consumers the right to opt-out of:

- The sale of their personal data.
- Targeted advertising.
- Automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements (profiling), if it will produce legal or similarly significant effects for a consumer.

(Colo. Rev. Stat. Ann. § 6-1-1306(1)(a); see Controller Obligations.)

The CPA Rules require businesses that engage in profiling to:

- Designate a method that permits consumers to opt out (4 Colo. Code Regs. § 904-3:9.04(D)).
- Provide consumers with a notice that includes:
  - what decisions are subject to the profiling;
  - the categories of personal data that it will use as part of the profiling;
  - a non-technical, plain language explanation of the logic it uses in the profiling process and how it uses profiling in the decisionmaking process, including any human involvement;
  - if it has evaluated the system for accuracy, fairness, or bias, including the impact of sensitive data, and the results of the evaluation;
  - the benefits and potential consequences of the decision based on the profiling; and
  - information about how consumers may exercise their right to opt out of the profiling.

  (4 Colo. Code Regs. § 904-3:9.03(A).)

- Conduct a data protection impact assessment if the proposed profiling presents a reasonably foreseeable risk of:
  - unfair or deceptive treatment of, or unlawful disparate impact on consumers;
  - financial, physical, or other substantial injury to consumers; or
  - a physical or other intrusion upon a consumer's solitude, seclusion, or private affairs or concerns, if it would be offensive to a reasonable person.

  (4 Colo. Code Regs. § 904-3:9.06(A); see Data Protection Impact Assessments.)

The CPA Rules permit a business to deny a consumer request to opt out of profiling if there is human involvement in the automated processing, which means a human with the authority to change or influence the processing's meaningfully considers the available data used in the processing or any resulting output (4 Colo. Code Regs. § 904-3:2.02). However, it must provide another notice that includes the information listed above plus information on how the consumer can correct or delete the personal data it used in the profiling. (4 Colo. Code Regs. § 904-3:9.04(C).)

The CPA also requires businesses to honor universal opt out mechanisms, such as a browser setting, that clearly communicate a consumer's affirmative, freely given, and unambiguous choice to opt out of personal data processing for targeted advertising or the sale of their personal data. The CPA Rules spend several pages setting out the technical specifications for how browsers and devices should offer and implement these signals, but delay compliance with this requirement until July 1, 2024. The CPA Rules also contemplate that by January 1, 2024 the CO AG will publish a list of mechanisms that businesses must honor, which creates some risk that the controls will be different in Colorado than in other states such as California and Connecticut. (4 Colo. Code Regs. §§ 904-3:5.01 to 5.09.)

Notably, Colorado removed provisions from an earlier version of the rules that contemplated the CO AG creating a state-wide do not sell registry, which would have been challenging to operationalize in places where the only way to opt out an individual is to contemporaneously place a cookie on their device.

Restrictions on Data Use

The CPA and the CPA Rules create personal data use restrictions that require controllers to:

- Limit personal data processing to the purposes they disclose in a privacy policy and what is necessary, adequate, and relevant for those purposes (see Purpose Specification and Data Minimization).
- Obtain opt-in consent for any sensitive data processing unless an exception applies (see Sensitive Data).
- Obtain parent or guardian consent when processing children's personal data or operating a website or business directed to children (see Children's Data).

These concepts are not new, as other states' laws also contain consent requirements for processing sensitive data and data minimization and purpose limitation requirements. However, the CPA Rules include a significant level of detail that will require businesses to work towards establishing comprehensive data governance policies. The CPA Rules' details also demonstrate that this may be an area of regulatory focus in the future.

Purpose Specification and Data Minimization

The consumer-facing disclosure requirements of the CPA are substantially the same as Virginia's and similar to the CCPA's. The CPA requires businesses to post a privacy policy detailing how they process personal information, but the CPA Rules add additional duties requiring businesses to line up collection and use in a more detailed and linear way than the other state laws. The CPA Rules also include requirements related to the privacy notice's accessibility, readability, and comprehensibility.

The CPA Rules on purpose specification and data minimization push businesses to take a granular approach when tracking processing activities and explaining them to consumers in a privacy policy. For example, businesses must specify the express purposes for which they collect and process each category of personal data, both in their privacy notices to consumers and internal documentation. The CPA Rules further prohibit controllers from using singular, broad purposes to justify unrelated or future processing activities, emphasizing the specificity requirements. This obligates businesses to use the specified personal data categories only for the expressly listed purposes and update their disclosures if those processing purposes change or evolve. Businesses must draft consumer disclosures with enough detail to provide a meaningful understanding of how the business uses each personal data category. (4 Colo. Code Regs. § 904-3:6.06.)

The CPA Rules also require businesses to conduct and document a data minimization analysis of **each** processing activity to assess whether the activity uses only the minimum

personal information necessary, adequate, and relevant for the express purpose. Businesses must also set a time limit for personal data erasure or conduct a periodic review. Biometric identifier use must receive annual, documented reviews to determine whether continued retention also of the data is necessary, adequate, and relevant to the processing purpose. (4 Colo. Code Regs. 904-3:6.07.)

Sensitive Data

Though Colorado takes the same opt-in approach to sensitive data as Virginia, the CPA Rules set a higher bar for establishing valid consent, requiring it to be:

- Obtained through the consumer's clear, affirmative action.
- Freely given.
- Specific.
- Informed.
- Reflective of the consumer's unambiguous agreement.

(4 Colo. Code Regs. § 904-3:7.03.)

The Rules also specify that businesses that collected sensitive data before July 1, 2023 must obtain consent to continue processing it unless the previously provided consent meets the above requirements. (4 Colo. Code Regs. § 904-3:7.02(B).)

The CPA Rules also create the new concept of sensitive data inferences and set out special rules for processing this type of data without consent (4 Colo. Code Regs. § 904-3:6.10(B)). Sensitive data inferences are inferences that a business makes based on personal data that it uses to indicate an individual's:

- Racial or ethnic origin.
- Religious beliefs.
- Mental or physical health condition or diagnosis.
- Sex life or sexual orientation.
- Citizenship or citizenship status

For example, if a business uses web browsing data alone or in combination with other personal data to infer a person's sexual orientation, the CPA Rules also consider the web browsing data to be sensitive data due to the inference made (4 Colo. Code Regs. § 904-3:2.02.)

The CPA Rules permit businesses to process sensitive data inferences about individuals over the age of 13 without consent if:

- The purpose of the processing is obvious to a reasonable consumer based on the context of the collection, the use of the personal data, and the consumer's relationship with the business.
- The business deletes both the underlying personal data and the sensitive data inferences within 24 hours of collection or completion of the processing activity, whichever occurs first.
- The business does not transfer or sell the sensitive data inferences or share them with any processors, affiliates, or third parties.
- The business does not process the personal data and sensitive data inferences for any secondary purpose.

(4 Colo. Code Regs. § 904-3:6.10(B).)

Since the prohibition on sale or sharing would remove the ability to rely on this exception for most advertising activities, it is unclear what use case this section is meant to enable.

Children's Data

Like Virginia's law, the CPA Rules require businesses to obtain consent from a child's parent or guardian when:

- Processing personal data related to a known child under the age of 13.
- Operating a website or business directed to children.

(4 Colo. Code Regs. § 904-3:7.06.)

On its face, this requirement goes beyond the consent requirement of the federal COPPA, which applies to personal data collected from a child via an online service. However, the Colorado and Virginia laws' consent requirements are subject to the same broad exceptions for sensitive data related to adults (see Sensitive Data). Confusingly, Colorado also fully exempts from the law any information regulated by COPPA, though this may have little practical effect given the similarities between COPPA and CPA compliance processes. For more information on COPPA, see Practice Note, Children's Online Privacy: COPPA Compliance.

Businesses should also note the significant differences in how state consumer privacy laws regulate processing children's data, for example:

- Colorado and Virginia do not require consent to process personal data of children over the age of 13 unless the processing involves sensitive data (Colo. Rev. Stat. Ann. § 6-1-1308(7); Va. Code Ann. § 59.1-578(A)(5)).

- Connecticut has the same consent requirement as Colorado for processing personal data of a known child under 13, but it adds a requirement to obtain consent from consumers aged 13, 14, or 15 before selling their personal data or using it for targeted advertising (Conn. Gen. Stat. Ann. § 42-520(a)(4), (7)).
- California takes a different approach and requires parent or guardian consent to sell or share personal data of children under 13, but not to collect it or use it for the business' internal processing activities (though COPPA still applies). California also requires consent from children over 13 and under 16 to sell or share their data, but it does not require any consent for its collection or internal processing. (Cal. Civ. Code § 1798.120(c), (d); Cal. Code Regs. tit. 11, §§ 7028, 7070, and 7071.)
- Utah and Iowa will require consent for sale or sharing or use for targeted advertising, but only when COPPA would already require it (Utah Code § 13-61-302(3); Iowa Code Ann. § 715D.4(2)).

Data Protection Impact Assessments

Both Colorado and Virginia require businesses to conduct data protection assessments (DPIAs) when a processing activity presents a heightened risk of harm to consumers (Colo. Rev. Stat. 6-1-1309(1); Va. Code. Ann. § 59.1-580(A)). However, businesses that drafted DPIAs ahead of the January 1, 2023 Virginia effective date should review them to ensure that they comply with the CPA Rules' extensive and detailed requirements.

The CPA Rules require controllers to:

- Conduct a DPIA before beginning a processing activity that presents a heightened risk of consumer harm.
- Involve all relevant stakeholders in the controller's organization and external parties where appropriate.
- Consider the scope of the risk, the size of its organization, the amount and sensitivity of the personal data it processes, and other factors when determining the DPIA's scope, depth, and detail.
- Update the DPIA as often as appropriate considering the personal data at issue and the level of risk, though at least annually if the DPIA relates to profiling in furtherance of decisions that produce legal or similarly significant effects for a consumer.
- Retain DPIAs, including prior versions, in electronic, transferable form for at least three years after the processing activity concludes.
- Provide a DPIA to the CO AG within thirty days of its request.

(4 Colo. Code Regs. §§ 904-3:8.02, 8.05 and 8.06.)

While the CPA does not require organizations to conduct retroactive DPIAs for processing activities underway before July 1, 2023, the CPA Rules require controllers to conduct a new DPIA if they modify an existing processing activity and materially change the level of risk (4 Colo. Code Regs. § 904-3:8.05(D)).

The CPA Rules require DPIAs to represent a genuine and thoughtful analysis of the risks and benefits of a processing activity that:

- Identifies and describes the risks to the consumer.
- Documents the measures the organization has considered and taken to address and offset the risks.
- Contemplates the benefits of the processing.
- Demonstrates that the processing's benefits outweigh the risks with the safeguards in place.

(4 Colo. Code Regs. § 904-3:8.02(A).)

In addition, the Rules set out 13 different pieces of information that a DPIA must contain, including:

- A short summary of the processing activity.
- The categories of personal data and whether they include sensitive data.
- The context of the processing activity, including the controller's relationship with the consumer and reasonable consumer expectations.
- The nature and operational elements of the processing activity, considering:
  - the type, amount, sources, and sensitivity of the personal data;
  - the technology and processors involved;
  - the personal data recipients and the associated processing purpose; and
  - operational details of the processing such as the planned processes for personal data collection, use, storage, retention, and sharing.
- The core purposes of the processing activity and any benefits that may result for the controller, consumer, the public, and other stakeholders.
- The sources and nature of the associated risks to consumers that the processing presents, for example:
  - constitutional, intellectual or physical privacy, data security, or discrimination related harms;
  - unfair, unconscionable, or deceptive treatment;
  - a negative outcome related to an individual's eligibility for certain rights, privileges or benefits such as

financial or lending services, housing, insurance, education, employment, criminal justice, healthcare, or access to essential goods and services;

- financial or economic harm; or
- physical injury, harassment, threats, or psychological harm.

- Safeguards the controller will use to reduce the identified risks, including:
  - using deidentified data;
  - measures the controller takes to comply with its duties under the CPA (see Controller Obligations), including data security practice, security assessments, and steps to comply with the CPA Rules' consent requirements; and
  - measures the controller takes to facilitate consumer rights.
- A description of how the processing's benefits outweigh the risks with the safeguards in place, including contractual agreements addressing data security and any other practices, policies, and trainings that mitigate risk.
- If a controller will process personal data for profiling purposes:
  - the specific types of personal data that the controller will use in the profiling or decisionmaking process;
  - the decision the controller will make using profiling;
  - the benefits of automated processing over manual processing for the stated purpose;
  - a plain language explanation of why the profiling directly and reasonably relates to the controller's goods and services;
  - an explanation of the training data and logic the controller used to create the profiling system, including any statistics it used in the analysis, whether created by the Controller or provided by a third party;
  - if the controller conducts the profiling through a third party software it purchased, the name of the software and copies of any internal or external evaluations of the software's accuracy and reliability where relevant to the risks set out in Colo. Rev. Stat. Ann. § 6-1-1309(2)(a) (see Controller Obligations);
  - a plain language description of the outputs secured from the profiling process;
  - a plain language description of how the controller will use the outputs from the profiling process, including to contribute to a decision to provide or deny financial or lending services, housing, insurance, education, enrollment or opportunity, criminal justice, employment opportunities, healthcare services, or access to essential goods or services;
  - the degree and details of any human involvement in the profiling process;
  - how the controller evaluates the profiling system for fairness and disparate impact, and the results of any evaluation;
  - safeguards it uses to reduce the risk of identified harms; and
  - safeguards for any data sets resulting from the profiling.

  (4 Colo. Code Regs. § 904-3:9.06.)
- When relying on the CPA Rule's exception for obtaining consent to use sensitive data inferences, the details of the controller's process that ensures that it does not transfer the personal data and sensitive data inferences and that it deletes them within 24 hours of the processing activity.
- The internal and external parties that contributed to the DPIA.
- Details of any internal or external audit related to the DPIA.
- The names, positions, and signatures of the individuals that reviewed and approved the DPIA and the approval dates.

(4 Colo. Code Regs. § 904-3:8.04.)

How Businesses Can Best Prepare for Compliance

The CPA changes the privacy compliance landscape in some meaningful ways. Whereas California's original consumer state privacy law required transparency and adherence to certain consumer rights with no explicit data management obligations, the CPA shifts the focus to data governance. Businesses must create a true privacy program, both to comply directly with the CPA and manage multiple processes and workstreams to account for the differences between the CPA, other state privacy laws, and even the EU General Data Protection Regulation (GDPR), if applicable.

Businesses that comply with California's and Virginia's laws will likely not find many Colorado requirements that are completely new. Rather, the compliance burden associated with the CPA and the CPA Rules arises from:

- The time required to identify and reconcile the nuances across the different state laws.
- The strategic effort required to mature the business' privacy program to govern personal data processing in line with Colorado regulator expectations.

Specifically, businesses working towards CPA compliance should focus on:

Creating a robust inventory of their processing activities, the personal information involved in each activity, and a process to ensure they update the inventory on a regular basis.

- Identifying which of their processing activities are high risk, for example, profiling, processing sensitive data, and selling and using personal data for targeted advertising, and prioritizing data minimization and risk mitigation for these activities.
- Creating a detailed process through which they offer, review, and honor sales and targeted advertising opt-outs, including:
  - ensuring that they identify all relevant processing activities;
  - they present options to consumers clearly;
  - the presentation aligns with the opt-out's technical implementation, for example, using a form when an opt-out cookie is more appropriate; and
  - investigating whether they require a consent management platform for their website if they do not already have one. Since California's law requires businesses to honor the Global Privacy Control (GPC) which is quickly becoming the standard for user-enabled privacy control, it is likely GPC will be an approved universal opt-out mechanism in Colorado.
- Evaluate whether they want to create many different processes for consumers to exercise their applicable state law privacy rights, align the states against certain common denominators, or expand rights to all consumers nationwide. Certain rights may be difficult to offer on a state-by-state basis, for example, if the only way to prevent a sale is to set an opt out cookie on the device of an unknown individual, it may be impossible to determine which requestors live in an eligible state.