



COLORADO PRIVACY ACT (CPA)

CHECKLIST



USERCENTRICS

Colorado Privacy Act (CPA) gives Colorado residents rights over how their personal data is collected and used.

This checklist walks through steps that support your compliance efforts under the Act, along with recommended best practices for privacy-related user experience.



Important to know:

Action	Date
Effective date	July 1, 2023
Retroactive	No
2025 amendment	Minors' consent provision now covers any consumer under 18 (previously narrower)

Note: A separate Colorado [biometric identifiers law](#) (not a CPA amendment) expanded consent requirements for biometric processing, covering both consumers and employees. This as an adjacent obligation, not part of the CPA itself.

1 Determine If Your Company Is Required to Comply

If your for-profit organization:

- Processes the personal data of at least 100,000 Colorado consumers, or
- Processes the personal data of at least 25,000 Colorado consumers, and receives a discount on goods or services from selling personal data

There is no revenue threshold. Consumer health data provisions apply to any business regardless of scale, with no threshold at all.

Exemptions include:

- Government agencies (state and local)
- Higher education institutions
- Air carriers
- National securities associations
- [GLBA](#)-regulated financial institutions and affiliates
- [HIPAA](#)-covered data (data-level, PHI only)
- [FCRA](#)-regulated consumer report data
- FERPA-regulated education data
- DPPA-regulated driver data
- [COPPA](#)-regulated data
- Certain employment records and job-applicant data

2 Create a Comprehensive Privacy Policy

Businesses are required to inform consumers at or before the point of data collection:

- Categories of personal data processed
- Purposes for which data is processed
- Categories of personal data the controller shares with third parties, if any
- Categories of third parties the controller shares personal data with, if any

Rights: Inform website visitors of their privacy rights and how to exercise them, including contact information and how a consumer may appeal a controller's decision.

Language: Keep the privacy policy clear and easy to understand.

Implementation: As a best practice, pair the privacy notice with an opt-out mechanism. For example, use a banner or pop-up when visitors visit your site, powered by a consent management platform (CMP).

3 Inform Consumers About Their Rights

Consumers' rights under the CPA:

- **Right to access:** Request and receive confirmation of whether a controller is processing their personal data
- **Right to correction:** Updates or corrections to inaccuracies in personal data collected
- **Right to deletion:** Personal data collected about them (with exceptions)
- **Right to data portability:** A copy of personal data in a portable, readily usable format

- **Right to opt out:** Of processing for the purposes of sale, targeted advertising, or profiling for decisions with legal or similarly significant effects
- **Right to non-discrimination:** For exercising privacy rights
- **Right of minors:** Consent must be obtained from a parent/guardian if the data subject is a minor (under age 18)
- **Right to restrict use of sensitive personal information:** Limit or refuse collection or use of personal data the law classifies as sensitive

4 As a Best Practice, Review and Update Your Privacy Policy or Notice Every 12 Months

Review operations and potential legal changes at least every 12 months. Update the [privacy policy](#) and its effective date, even if no other changes are made.

Transparency: Keep the information visitors must be notified about clear, comprehensive, and up to date, with the last-update date clearly visible. A [Privacy Policy Generator](#) can help.

Data sold: List all categories of personal information your business has sold in the past 12 months.

5 Enable Clear Options When Consent Is Required

If the personal data collected is sensitive, or that of a minor, make information and options clear and easily accessible on your website, e.g., [via a CMP](#).

6 Authenticate Consent or Opt-Out for Collection of Sensitive Personal Data or Data From Minors

Sensitive personal data: Provide clear options to opt out and store preferences for processing [sensitive personal data](#).

Consent for children: Obtain consent from a parent or legal guardian for collection of personal data if the data subject is 18 or younger.

7 Enable and Respond to Data Subject Access Requests (DSARs)

Provide one or more contact options (e.g., toll-free phone number, web form, email). Set up a system to enable submission, verification, and tracking of [DSARs](#). If identity cannot reasonably be verified, inform the consumer and explain why, and enable them to rectify. Keep records of all requests and responses for 2 years.

Respond within 45 days from the date the request is received, extendable by an additional 45 days if the business notifies the consumer of the extension and its reason within that first 45-day window.

Falling thresholds, rising enforcement and litigation, eroding ad revenue. Do you know your risk?

GET IN TOUCH