usercentrics

# California Consumer Protection Act (CCPA) and California Privacy Rights Act (CPRA) Checklist

These steps will help you achieve compliance with the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), which apply to and protect residents of California. The checklist also includes recommended best practices for data privacy-related user experience.

## 1 Determine if your company is required to comply

If your for-profit organization:

- has gross annual revenue that exceeds US $25 million for the preceding year, or
- buys, sells or shares personal data from 100,000+ California consumers or households annually, or
- derives at least 50% of annual revenue from selling or sharing the personal data of California consumers

**Important to know:**

The CCPA was expanded and amended by the CPRA, which came into effect January 1, 2023. From July 1, 2023, it applies retroactively to the processing of personal data back to January 1, 2022.

## 2 Create a comprehensive Privacy Policy

**Purpose:** Inform consumers at or before the point of data collection:

- how data is collected
- how long collected data is retained
- categories of personal data collected
- purposes for which data is collected
- whether data collected is sold to or shared with third parties
- the third parties with which data is shared

**Rights:** Inform website visitors of their privacy rights and how to exercise them.

**Language:** Ensure the Privacy Policy is clear and easy to understand, which includes availability in the languages in which your business provides information in California.

**Implementation:** Implement a privacy notice with information about data use, consumers' rights and user options, like consent opt out. Enable consumers to exercise rights, like opting out, via a banner or pop-up when users visit your site, e.g. with a Consent Management Platform.

## 3 Inform users about their rights

**Consumers' rights under the CCPA:**

- **Right to Know:** what personal data is collected and how it is used or shared
- **Right to Delete:** personal data that has been collected about them (with exceptions)
- **Right to Data Portability:** copy of personal data must be provided in a portable and readily useable format
- **Right to Non-discrimination:** for exercising privacy rights
- **Right to Opt Out:** of the sale or sharing of their personal data
- **Right of Minors:** consent must be obtained from a parent/guardian before children's personal data is collected

**Additional rights under the CPRA:**

- **Right to Correction:** updates or corrections to inaccuracies in personal data collected
- **Right to Know about Automated Decision-making:** request information about automated decision-making and likely outcomes of using it, specifically with regards to profiling
- **Right to Opt Out of Automated Decision-making:** refuse use of automated decision-making technology with regards to personal data
- **Right to Restrict Use of Sensitive Personal Information:** limit the collection or use of personal data the law classifies as sensitive

## 4 Review and update your Privacy Policy every 12 months

**Review your operations** and potential changes in the law every 12 months. Update your Privacy Policy information and its **effective date.** Effective date should be updated even if you don't make any other changes to the Policy.

**Transparency:** Ensure that the information that users must be notified about is clear, comprehensive and up to date. Ensure that the date of the last update is clearly visible.

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

## 5 Re-offer opt in consent every 12 months

If the consumer has opted out, you can present the option to opt in again **after 12 months.**

## 6 Include a clear and conspicuous "Do Not Sell Or Share My Personal Information" link (opt out)

**Availability:** Easily accessible on your website homepage.

**Method:** Via the use of a Consent Management Platform (CMP).

## 7 Authenticate consent for collection of sensitive personal data or data from minors

**Sensitive Personal Data:** Provide a clear "Limit The Use of My Sensitive Personal Information" link to enable opt out.

**Minors' Consent:** Obtain explicit consent (opt-in) from the data subject before processing the personal data if the data subject is between the ages of 13 and 16.

**Parents/Guardians:** Obtain consent from a parent or legal guardian for collection of personal data if the data subject is 13 or younger.

## 8 Enable consumers to make Data Subject Access Requests (DSARs)

Provide at least **2 contact options,** e.g. toll-free phone number, web form, email.

**Set up a system** to enable submission of DSARs.

## 9 Set up a system to verify Data Subject Access Requests (DSARs)

Enable consumers to **attach documentation** when submitting a request, to enable secure verification of their identity and residency.

**Set up a system** to enable submissions for verification requests.

If your business c**annot reasonably verify** the consumer's identity to the appropriate degree of certainty, it must **inform the consumer and explain** why the request could not reasonably be verified, and enable the consumer to rectify.

## 10 Keep track of Data Subject Access Requests (DSARs)

**Set up a system** to track all requests.

**Time period:** keep records of all requests and your business responses **for 2 years.**

## 11 Fulfill Data Subject Access Requests (DSARs)

Standard time period: **within 45 days.**

Extended time period: **up to 90 days.**