



CCPA Compliance Checklist

1

CREATE PRIVACY POLICY

MAINTAIN A DATA INVENTORY

2

3

IMPLEMENT PROTOCOLS TO ENSURE CONSUMER RIGHTS

CREATE A DO NOT SELL MY PI BUTTON

4

5

TAKE NECESSARY REMEDIATION ACTIONS

GIVE CONSUMERS THE RIGHT TO ACCESS THEIR PI

6

7

OBTAIN CONSENT FROM MINORS

UPDATE SECURITY ISSUES

8

9

UPDATE THIRD-PARTY PROCESSOR CONTRACTS

PERFORM TRAINING

10



The California Consumer Privacy Act (CCPA) is a data privacy law that regulates the collection, managing, processing, and selling of the personal information of California residents. It went into effect on January 1, 2020. The CCPA privacy law regulates any business, that collects **personal information (PI) from California consumers**, including businesses based outside of the United States.

The CCPA law applies to businesses that conduct business in California and meet one of the following criteria:

- **Sales of consumer data account for 50% (or more) of annual revenue**, regardless of total revenue.
- **Your business has total revenues of over \$25 million**, even if the sale, receipt, or purchasing of personal information is only a small percentage of your business's total revenues or business activities.
- **Your organization sells, rents, receives or purchases consumer information on 50,000 (or more) individuals** within a given calendar year (365 days).

NOTE

The CCPA was followed by the California Privacy Rights Act (CPRA), that amends existing provisions by creating new and expanded rights for California consumers and increasing obligations on businesses. The CPRA went into effect on January 1, 2023.

Read this CCPA compliance checklist to learn more about:

- Users' rights under the CCPA.
- Businesses' responsibilities under the CCPA.
- How to get and store valid user consent.
- What information your cookie banner needs to provide.
- What information your Privacy Policy needs to provide.
- How to comply with the CCPA.
- The benefits of using a Consent Management Platform (CMP).

DISCLAIMER

Content available on CookieScript is intended for general information purposes only- it is not legal advice. Therefore, before taking any actions based upon information provided by CookieScript, we encourage you to consult with a lawyer or an attorney licensed in the relevant jurisdiction(s).

Consumers' Main Rights under the CCPA:





- 🔒 **Right to notice.** Consumers have the right to know what personal data is being collected about them and the purposes for which the information is being used.
- 🔒 **Right to know.** Consumers have the right to know the third parties with whom the business shares the information and whether their personal data is sold or disclosed.
- 🔒 **Right to disclosure.** Consumers have the right to access their personal data upon request.
- 🔒 **Right to opt-out.** Consumers have the right to agree or disagree to collect, manage, or sell their personal data.
- 🔒 **Right to deletion.** Consumers have the right to ask for the deletion of their personal data.
- 🔒 **Right to equal services and prices.** Consumers must not be discriminated against for exercising their privacy rights.

NOTE: Be mindful of consumers' age. The CCPA offers extended protection for consumers under the age of 16. If a business knowingly collects information regarding a consumer's age, the commercial entity is prohibited from selling that person's information without express consent from the individual or the individual's parent or legal guardian. Children under the age of 13 require the consent of a parent or guardian.

Consumers' Rights under the CPRA

In 2023, the CCPA was followed by the California Privacy Rights Act (CPRA).

Under the CPRA, California consumers have the following new rights:

-  **Right to opt-out of sharing sensitive personal information.** California consumers may restrict the use and disclosure of sensitive personal information for certain secondary purposes to third parties for cross-context behavioral advertising, which essentially refers to interest-based advertising.
-  **Right to opt-out of automated decision-making technology.** California consumers could request to opt-out of the use of automated decision-making technology in connection with decisions related to the economic situation, health, personal preferences, interests, behavior, geo-location, racial or ethnic origin, religious or philosophical beliefs, etc.
-  **Right to access information about automated decision-making.** California consumers could request access to information about how the automated decision-making processes are performed and access to a description of the likely outcome based on that process.
-  **Right to correction.** California consumers can request correction of their personal data held by a business if that data is inaccurate.

- 🔒 **Right to opt-out of certain uses and disclosures of sensitive personal information.** Sensitive personal information could refer to the following information: consumer's account log-in details; financial account, debit card, or credit card number in combination with a security or access code, password, or credentials; social security number, driver's license, state ID card, or passport number; precise geo-location; racial or ethnic origin, religious or philosophical beliefs, or union membership; the contents of a consumer's email and text messages unless the business is the intended recipient of the communications; genetic data and biometric data; health, sex life or sexual orientation.
- 🔒 **Rights for children.** A company must obtain **explicit** (opt-in) consent before selling or sharing the personal information of a consumer under 16. The consent should be specific, freely given, informed, and unambiguous.
- 🔒 **Right to data portability.** California consumers can request businesses to transmit their personal information or a part of it to another company. CPRA also points out that the data should be provided in a format easily understandable and in a commonly used, machine-readable format.

NOTE: Right to know, right to delete, and right to opt-out remain the same in both the CCPA and the CPRA. California consumers have the right to access and delete their personal information and to opt-out of the sale or sharing of their personal data.

1. Create Privacy Policy

Create Privacy Policy that complies with CCPA and **update it at least once every 12 months.**

Updating your website's Privacy Policy helps to build customer trust in your business and how you use customers' data.

Google's search algorithms also prefer websites with unique privacy policies, and this is factored into websites' trustworthiness.

The Privacy Policy is the most significant compliance requirement for businesses under the CCPA compliance framework.

All businesses that collect, store, or process personal information must have a Privacy Policy.

The Privacy Policy should inform consumers:

- That you collect their personal information.
- How they can refuse your access to their personal information.
- What are you planning to do with their personal information.
- Why you collect this information.
- That you won't discriminate against them if they do not provide consent for you to use their personal data for marketing purposes.

2. Maintain a data inventory

Start by creating an inventory of what personal information you have collected from consumers. Examine the last year of your business' data activities, and especially how you use the data you collect. Conduct an inventory of consumer data held by your organizations, and those you share with third parties and vendors. This also means taking stock of so-called "offline" data, which might include personal details collected in person.

Assign a person or team to be responsible for data privacy and train your employees. The responsible person should focus on CCPA and other compliance standards and the consumers' personal information protection.

Companies must identify:

- Which data is used for the sale.
- What categories of personal information are transferred to third parties.
- Are there any categories of personal information, covered by HIPAA, the FCRA, or another law that would exempt the data from the CCPA's scope.
- When the data was collected. The consumers' personal data has to be kept for 12 months.

📌 The database has to be kept up to date and be able to track all consumer rights requests.

3. Implement protocols to ensure consumer rights

California's consumers have these main rights under the CCPA:

- Right to notice.
- Right to know.
- Right to disclosure.
- Right to opt-out.
- Right to deletion.
- Right to equal services and prices.

Inform consumers before or at the point of data collection that you want permission to collect their personal information. The consent notice should inform about the PI collected and the purpose for which this information is being collected.

! The notice should also include a link to the company's Privacy Policy.

NOTE: You must respond to consumer requests. If California residents requested a detailed account of what information was collected on them over the span of the last 12 months or requested to delete their personal data- provide the information or delete it, correspondingly.

4. Create a Do Not Sell My PI button

Create a **Do Not Sell My Personal Information** button on a cookie banner or a separate web page if you sell personal information.

i California's consumers should have an option to prevent selling of their information, if they wish.



5. Take necessary remediation actions

Implement a system that allows certain data to be **immediately** and **securely** purged in response to requests deriving from consumers at the individual level.

📌 Remediation does not always mean the deletion of personal data.

Adequate action should depend on the type of sensitive data your organization is processing.

In response to consumers' requests', you could **delete**, **organize differently** or **migrate** data to other locations for the best fit of consumers' needs adhering to compliance regulations.



6. Give consumers the right to access their PI



Give consumers the right to access their personal information. Allow users to verify their identification and access their personal data held by organizations. The verification system should be a part of the Privacy Policy.



Provide consumers with several ways to request their personal information, for example via a phone, or via a web page.



Provide all the required personal information within 45 days. If PI was sold to third parties, inform the consumer the customers about the sold information, its collection purpose, and the categories of third parties the data was sold to.

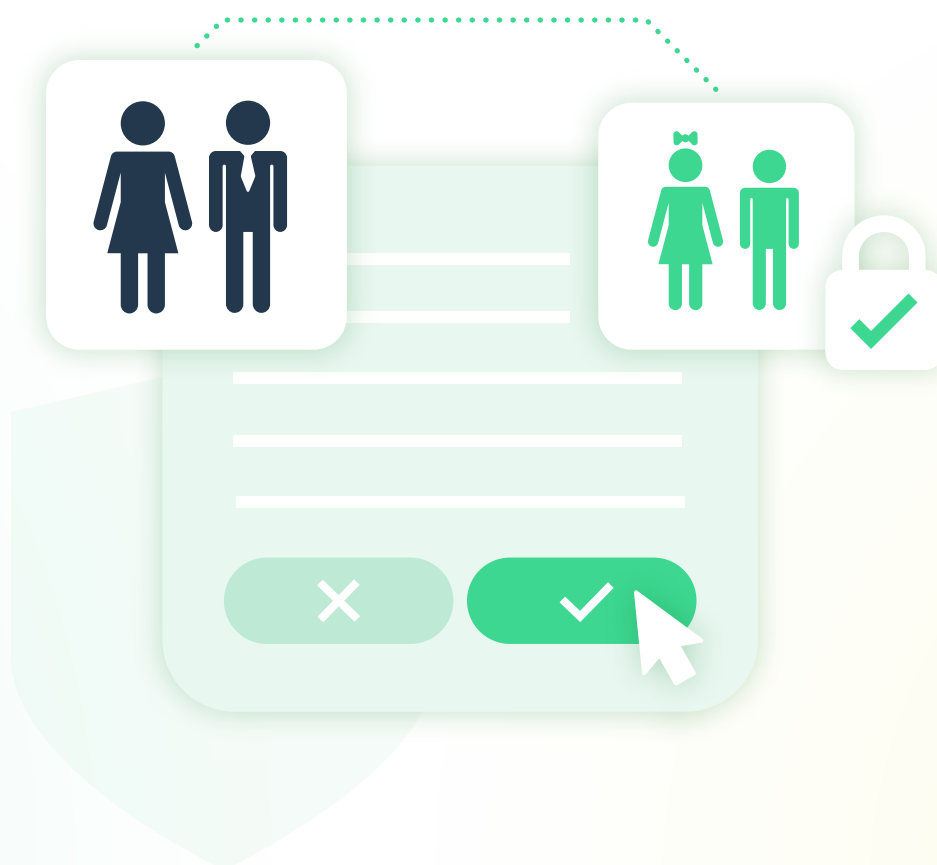


Give consumers the right to request deleting their personal information.

7. Obtain consent from minors

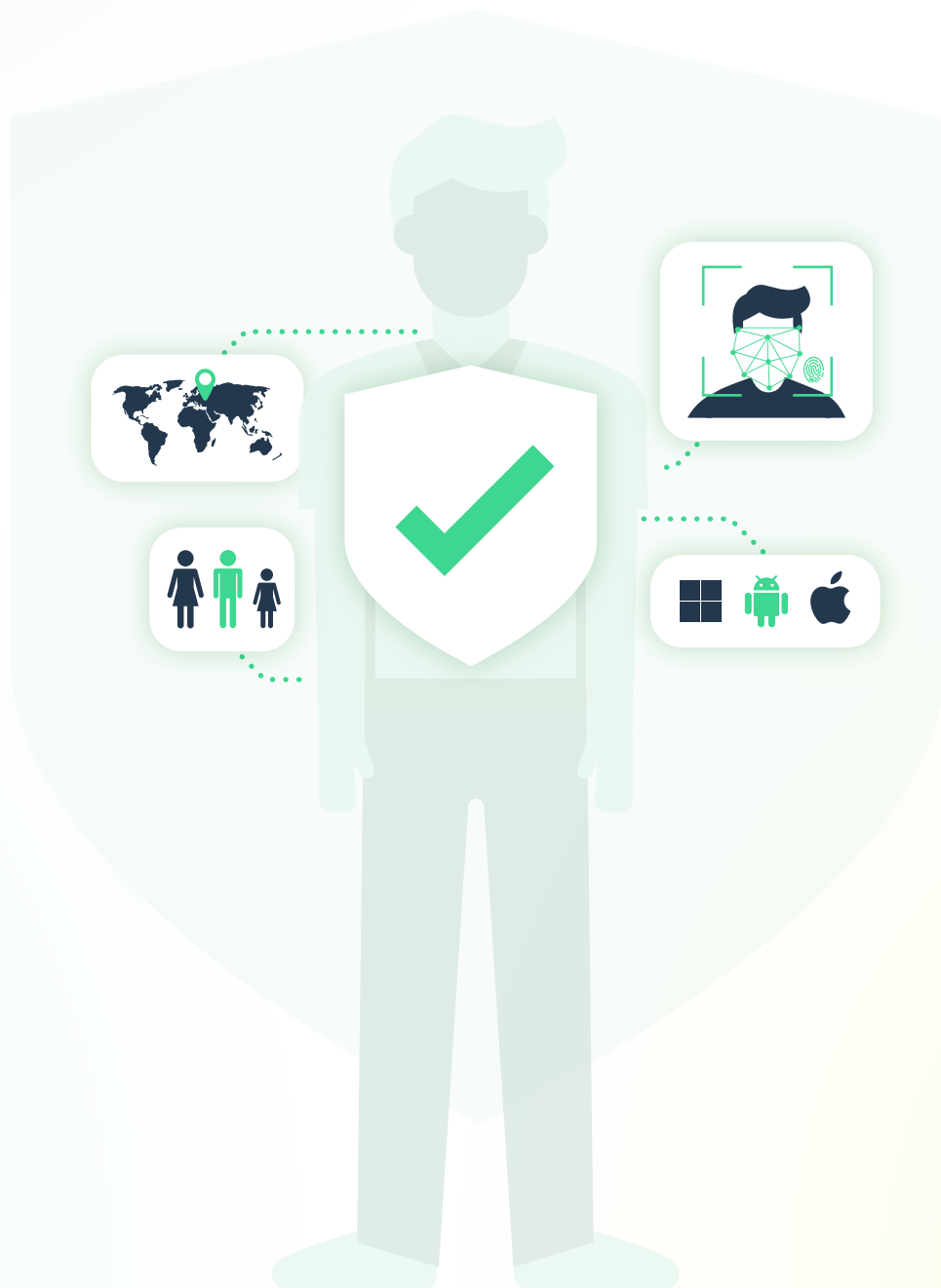
Minors **under the age of 16** need to give explicit consent to process their personal data since minors do not automatically consent under the CCPA.

Develop a process to obtain direct consent from minors aged 13-16 years, and a process to obtain parents' consent from minors **under 13 years**.



8. Update security issues

The CCPA requires businesses to protect personal data with **“reasonable” security**. It means that personal data should be kept “reasonably” confidentially and should not be made available to non-related parties.



9. Update third-party processor contracts



If businesses use other companies to process personal data collected by them, businesses need to **update their third-party contracts** regarding consumers' personal data.

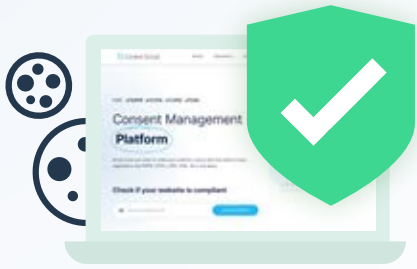
10. Perform training

The CCPA requires that employees handling consumer personal data and related inquiries be informed of all CCPA requirements.

❗ **Companies must comply with CCPA regulations.**



Failure to comply with the CCPA could lead to fines, lawsuits, and reputational damage.



CookieScript CMP - Your Solution for CCPA compliance

Use CookieScript CMP to ensure GDPR compliance and mitigate risks associated with data processing activities.



CookieScript is trusted by top-level brands as well as startups and small companies.

It has the following functionalities:

- **Google-certified CMP.** CookieScript is a Google-certified CMP partner and comes with a full IAB TCF v2.2 integration.
- **Supports Google Consent Mode v2.** If you want to use Google services (GA4, Google Ads, gtag, and Google Tag Manager) in the EU or EEA, you need to use a Google-certified CMP.
- **Local Storage and Session Storage scanning and blocking.** GDPR and other privacy laws require blocking of cookies, Local Storage and Session Storage until user consent is given. However, majority of CMPs do not offer this functionality. CookieScript blocks both Local Storage and Session Storage.
- **Fully customizable.** CookieScript CMP allows Cookie Banner behavior adjustments, and design customization, and has a self-hosted code option.

- **Multiple integrations.** CookieScript CMP integrates easily with Google services automatically via Google Tag Manager, so you could use Google advertisement products easily. The CookieScript CMP is also integrated with other platforms, including content management systems such as Drupal, Magento, Shopify, WordPress, PrestaShop, etc., and analytics platforms, including Google Analytics 4.
- **Language and jurisdiction support.** CookieScript Cookie Banner and cookie declaration report is translated into 40+ languages and has geo-targeting.
- **Easy to set up.** CookieScript CMP could be easily implemented in just a few steps in a privacy laws-compliant way using banner settings hints for different jurisdictions.
- **Full compliance solution.** CookieScript CMP comes with the Cookie Scanner, Privacy Policy Generator, script manager, and user consent manager. It blocks cookies, Third-Party Cookies, Local Storage and Session Storage, so you can be sure your website is compliant with the GDPR and other privacy regulations 100%!