16-Step CCPA compliance checklist

As you prepare to comply with CCPA, this checklist will provide a framework you can follow. Reading the checklist will help you understand the processes and controls you must implement. We'll also factor in guidelines added by the CPRA.

1. Develop a Privacy Policy

Data collectors need to write or update their privacy policy to meet CCPA guidelines.

Action Items:

- □ Create or update your privacy policy with CCPA guidelines in mind
  - □ Ensure your policy covers how you collect, use, share, and sell data
  - □ Include consumers' rights under the CCPA and how they can exercise them
- □ Put the policy on your home page or mobile app

2. Refine Your Data Governance

Data governance refers to the processes you rely on to keep data private, accurate, secure, and usable. The CCPA shapes how businesses approach data governance.

Action Items:

- □ Run an overall assessment of your data governance policies
- □ Include a cost/benefit analysis of any data-selling practices
- □ Prepare records of customer data to respond to customer requests quickly
- □ Honor Californians' requests to limit the use of their data

3. Audit Your Third-Party Exposure to CCPA Compliance

Most companies share consumer PI with third parties they partner with. The CCPA requires these third parties to also meet its standards.

Action Items:

- □ Ensure your third-party vendors comply with your company's PI protection policies, including:
    - □ Security practices
    - □ Data controls
  - □ Require third-party contracts to clearly define:
    - □ What data the vendors share
    - □ Why they share this data
    - □ How they share this data
- □ Update your contracts to prohibit vendors from using personal information outside the contractual relationship

4. Understand Your Exposure to Personal Information Regulation

Collecting unnecessary data increases a company's risk posture. To avoid penalties, check your PI collection processes.

Action Items:

- □ Audit your data collection processes to understand:
    - □ What PI you collect
    - □ How you store PI
    - □ Who has access to this PI
    - □ Which third parties you share this PI with
- □ Check the data you retain to ensure you meet:
    - □ Data minimization requirements
    - □ Data retention requirements

5. Prepare an Incident Response Plan

Whether as an independent process or part of an overall risk management plan, develop incident response procedures to handle CCPA violations.

Action Items:

- □ Plan responses to common incidents like:
  - □ Stolen personal information
  - □ Breakdowns in privacy practices
  - □ Corruption of data you hold
- □ Assign incident response responsibilities to specific stakeholders
- □ Perform regular simulations to stay prepared

6. Audit and Update Your Security and Data Protection Controls and Processes

Mitigate any weaknesses in your security and data protection practices.

Action Items:

- □ Improve processes for storing and transmitting customer data
- □ Set up safeguards against data breaches
- □ Encrypt all the personal data you retain

7. Implement Identity Verification Systems

CCPA compliance requires identity verification to learn a user's age and respond to their requests, so you must have processes in place to verify consumers' identities.

Action Items:

- □ Create a standardized process to verify a customer's identity
- □ Implement safeguards to keep people from accessing another person's PI

□ Implement measures to get consent from minors' parents after verifying their identity

8. Develop a Notice at Collection

Customers have a right to be informed of your business's data collection processes before data collection begins.

Action Items:

- □ Provide a notice at collection covering:
  - □ The categories of information you collect
  - □ Why you collect this data
  - □ Where you collect that data from
  - □ What kinds of third parties you share their information with
- □ Include a "do not sell link" for customers who don't want their data sold

9. Implement Systems to Support Consumers' Right to Know

Users have a right to request details about the PI collected from them. Organizations must honor these requests to know about this data collection.

Action Items:

- □ Protect the right to know by:
  - □ Providing an avenue for customers to access their PI
  - □ Making user PI reports understandable to the average consumer
  - □ Setting up processes to respond to requests within 45 days

10. Implement Systems to Support Consumers' Right to Delete

Customers have the right to delete information businesses have about them.

Action Items:

- □ Secure the right to delete by:

    - □ Giving customers the right to delete their PI
    - □ Letting customers correct inaccuracies in their PI
    - □ Making third parties delete shared customer data after a request

11. Implement Systems to Support Consumers’ Right to Opt Out

Users can opt out of the sale or sharing of their personal information.

Action Items:

- □ Give the right to opt out of data collection:
    - □ Build a webpage where customers can opt out
    - □ Embed a button on another webpage to opt out
- □ Wait 12 months before asking users to opt back into data collection

12. Implement Systems to Support Consumers’ Right to Nondiscrimination

Consumers have a right to fair treatment under the CCPA.

Action Items:

- □ Uphold the right to nondiscrimination:
    - □ Do not give any customers arbitrary preferential treatment
    - □ Do not punish customers who exercise CCPA rights

13. Offer Privacy Training for All Personnel

Your employees, especially customer-facing staff, need to understand users’ rights under the CCPA.

Action Items:

- □ You can train your employees on CCPA guidelines through:
    - □ Online courses
    - □ In-person training sessions

- □ Shared online documents with CCPA information

14. Use Automation to Monitor Compliance Continuously

Manually tracking CCPA compliance is impractical for companies above a certain size. Continuous compliance monitoring can help you meet CCPA standards.

Action Items:

- □ Get a continuous compliance platform that checks your compliance posture by:
  - □ Creating incident response plans for detecting, reacting, and reviewing past breaches
  - □ Conducting CCPA tests on your security processes
  - □ Storing documentation on data processing, data subject requests, consent records, and privacy impact assessments

15. Conduct independent risk assessments

High-risk organizations handling sensitive data need to conduct third-party risk assessments.

Action Items:

- □ Verify if the data you retain counts as “sensitive” or “high-risk” under CCPA guidelines
  - □ If so, conduct independent risk assessments via a third party
  - □ Schedule these assessments at least once a year

16. Incorporate Feedback to Improve CCPA Compliance Processes

Your CCPA compliance process must evolve with the regulatory and threat landscapes.

Action Items:

- □ Develop feedback mechanisms to incorporate learnings from compliance events
  - □ Conduct regular reviews of your CCPA data compliance program