COMPLIANCE CHECKLIST

CCPA / CPRA compliance checklist

California Consumer Privacy Act, as amended by the CPRA

Jurisdiction: Businesses subject to California consumer privacy law

Programme details

ORGANISATION NAME

[Organisation name]

ASSIGNED TO

[Assigned to]

TARGET COMPLETION DATE

[Target completion date]

REVIEWED BY

[Reviewed by]

REVIEW DATE

[Date]

Who CCPA / CPRA applies to

Businesses that do business in California and meet at least one CCPA threshold: $26,625,000+ in annual revenue (CPPA-adjusted as of 1 January 2025), 100,000+ California consumers / households, or 50%+ of revenue from selling personal information.

CCPA / CPRA checklist

STEP 1

- [ ] Confirm CCPA applicability and document the basis (revenue threshold - $26.625M+ as of 1 Jan 2025, consumer count of 100K+, or 50%+ revenue from sale of PI).

STEP 2

- [ ] Inventory the personal information you collect, the sources, the purposes, and disclosures.

STEP 3

- [ ] Publish a CCPA-compliant privacy notice covering all required disclosures (CCPA § 1798.100).

STEP 4

- [ ] Stand up a "Do Not Sell or Share My Personal Information" link and signal-honouring mechanism.

STEP 5

- [ ] Build the consumer rights request workflow - Know, Delete, Correct, Opt-Out, Limit Use of SPI.

STEP 6

- [ ] Implement identity verification proportionate to the request type and the data sensitivity.

STEP 7

- [ ] Update vendor agreements with service-provider / contractor / third-party terms.

STEP 8

- [ ] Train staff on intake, verification, and the 45-day response window (extendable by 45 days).

STEP 9

- [ ] Log all consumer requests, response times, and outcomes for the metrics report.

STEP 10

- [ ] Annual review and update for legislative or regulatory changes.

FAQ

Is the CPRA a different law from the CCPA?

The California Privacy Rights Act (CPRA) is a 2020 ballot measure that amended and expanded the CCPA, effective 1 January 2023. The combined regime is often called "CCPA / CPRA" or just "CCPA". The CPRA added rights (Correct, Limit Use of Sensitive PI), restructured "sale" into "sale or share", and established the California Privacy Protection Agency.

Do I need to honour Global Privacy Control (GPC) signals?

Yes. The CPPA has confirmed that businesses subject to the CCPA / CPRA must honour GPC signals as a valid opt-out of sale or share for the browser sending the signal.

What is the difference between a "service provider" and a "third party" under CCPA?

A service provider processes personal information on the business's behalf under a CCPA-compliant contract that restricts use to the disclosed business purposes. A third party is everyone else - and disclosure of PI to a third party is treated as a "sale" or "share" requiring opt-out. The vendor contract language is what determines which bucket a recipient falls into.

How long do I have to respond to a consumer rights request?

Confirm receipt within 10 business days; substantively respond within 45 calendar days. You can extend by an additional 45 days where reasonably necessary, with notice to the consumer.

Source: https://ba-copilot.com/compliance/ccpa-compliance-checklist. Tick each item as it is completed and add the named owner.