

California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA) — Cal. Civ. Code § 1798.100 et seq.



CCPA/CPRA is California privacy law giving residents what it is control over their personal data and requiring businesses to protect and disclose data practices.

The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), is a comprehensive state privacy regulation that helps organizations protect Californians' personal data and ensure transparency in data processing activities. Its primary aim is to give individuals greater control over how their personal information is collected, used, and shared by businesses.

Enforced by the California Privacy Protection Agency, this regulation applies to for-profit entities doing business in California that meet specific thresholds, such as revenue size or volume of data processed. The CCPA/CPRA covers key areas including data protection, privacy governance, consumer rights, risk management, and incident response requirements, aligning with other privacy frameworks like the EU GDPR.

At a glance

PUBLISHER California Privacy Protection Agency (CPPA)	TYPE Regulation	VERSION CCPA (2018) as amended by CPRA (2020)
EFFECTIVE January 1, 2023	DOMAIN Privacy	FAMILY Global Privacy Regulations
REGION California	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: https://cppa.ca.gov/regulations/pdf/20221102_mod_text.pdf

Why it matters

- **Strengthen privacy governance** Promote structured oversight and management of personal data, reducing risks associated with unauthorized access or mishandling.
- **Enhance regulatory alignment** Support consistent adherence to state and international privacy requirements, simplifying compliance efforts and legal reporting obligations.
- **Increase audit readiness** Enable organizations to systematically document data practices and consumer requests, improving preparedness for regulatory audits and investigations.
- **Support consumer trust** Boost public confidence by transparently communicating data practices and honoring individuals' rights over their personal information.

How SmartSuite supports CCPA/CPRA

Data Inventory and Classification

Document personal data categories, sources, uses, and sharing with traceability.

DSAR and Opt-Out Workflows

Manage access, deletion, correction, and opt-out requests with deadlines and evidence.

Vendor, Service Provider, and Contractor Oversight

Track contracts, restrictions, and monitoring for third parties handling personal data.

Notice, Consent, and Policy Governance

Manage notice content, policy reviews, and evidence that practices match statements.

Retention and Deletion Controls

Operationalize retention rules and deletion processes with proof of execution.

Compliance Reporting and Audit Trail

Report request performance, open issues, and accountability evidence.

Common framework mappings

- GDPR
- ISO 27701
- NIST Privacy Framework v1.0
- Singapore PDPA
- PIPEDA
- UK DPA 2018
- UK GDPR

Official resources

California Consumer Privacy Act and California Privacy Rights Act Regulations

Provides the latest official regulations for CCPA/CPRA as amended.
cpa.ca.gov/regulations/pdf/20221102_mod_text.pdf

CCPA/CPRA Initial Statement of Reasons

Describes the rationale behind the CCPA/CPRA regulatory amendments.
cpa.ca.gov/regulations/pdf/20220708_isr.pdf

California Privacy Protection Agency's CCPA/CPRA FAQs

Outlines key FAQs about compliance with CCPA/CPRA.
cpa.ca.gov/faq.html

California Office of the Attorney General's CCPA Information Page

Provides comprehensive resources and guidance related to CCPA.
oag.ca.gov/privacy/ccpa

Frequently asked questions

What is CCPA / CPRA used for?

The CCPA / CPRA is designed to enhance the privacy rights and data protection of California residents by regulating how organizations collect, use, and share personal information. It requires businesses to enable consumer rights, improve transparency in data processing, and implement robust privacy governance practices.

Is CCPA / CPRA compliance mandatory for all organizations?

CCPA / CPRA compliance is mandatory for for-profit organizations that do business in California and meet certain thresholds, such as annual gross revenues above \$25 million, processing personal information of 100,000 or more consumers or households, or deriving 50% or more of their revenue from selling or sharing personal information. Companies outside California may still be subject if they target California residents.

What is the scope of CCPA / CPRA applicability?

The CCPA / CPRA applies to personal information collected from California residents by qualifying businesses, regardless of the organization's geographic location. The regulation excludes certain data sets, such as those covered by specific U.S. federal privacy laws, and generally applies only to for-profit entities meeting regulatory thresholds.

What are key compliance requirements and artifacts under CCPA / CPRA?

Key requirements include providing updated privacy notices, honoring consumer rights (access, deletion, correction, opt-out), maintaining records of data processing activities, conducting risk assessments related to sensitive personal information, and managing third-party data sharing agreements. Required artifacts include records of requests, processing inventories, and impact assessments.

How do organizations implement CCPA / CPRA controls?

Implementation involves data mapping to understand information flows, updating consumer consent mechanisms, deploying technical and administrative safeguards, establishing incident response processes, and creating governance policies. Continuous staff training and assigning roles for privacy oversight are also critical for effective compliance.

How does CCPA / CPRA relate to other privacy frameworks?

The CCPA / CPRA aligns with global privacy standards like the EU GDPR by emphasizing transparency, data minimization, and consumer rights. However, it has unique requirements tailored for California and features specific enforcement mechanisms and consumer rights distinct from other frameworks.

What are the ongoing compliance obligations under CCPA / CPRA?

Ongoing obligations include continually updating privacy notices, regularly assessing privacy risks, maintaining records of processing and consumer requests, monitoring third-party data sharing, and conducting periodic internal audits. Organizations must also respond to consumer rights requests within regulatory timelines.

How would SmartSuite support CCPA / CPRA?

SmartSuite supports CCPA / CPRA compliance by enabling organizations to track privacy risks, manage data protection controls, and document compliance evidence such as policies and request logs. Its features facilitate audit readiness through centralized dashboards, streamline reporting, and automate workflows for managing consumer rights, remediation tasks, and regulatory deadlines.

License included / downloadable: Yes The CCPA and CPRA are California state laws and are publicly available through official California government resources.

Full framework page and mappings: smartsuite.com/frameworks/ccpa-cpra-california-consumer-privacy-act-california-privacy-rights-act