



CCPA/CPRA Compliance Guide

A comprehensive guide to California privacy law compliance for businesses and nonprofits. Navigate CCPA and CPRA requirements with confidence and protect consumer privacy rights.

Understanding California Privacy Laws

CCPA (2018)

The California Consumer Privacy Act established foundational privacy rights for California residents, including the right to know what personal information is collected and the right to delete data.

- Effective January 1, 2020
- Covers businesses meeting specific thresholds
- Consumer-focused rights and transparency

CPRA (2020)

The California Privacy Rights Act expanded CCPA protections with stricter requirements, new consumer rights, and the creation of the California Privacy Protection Agency.

- Effective January 1, 2023
- Enhanced sensitive data protections
- New enforcement mechanisms

Does CCPA/CPRA Apply to Your Organization?

The law applies to for-profit businesses that collect California residents' personal information and meet at least one of these thresholds:

Annual Revenue

Gross annual revenues exceed **\$25 million** in the preceding calendar year

Data Volume

Buy, sell, or share personal information of **100,000 or more** California residents or households annually

Revenue from Data Sales

Derive **50% or more** of annual revenue from selling or sharing consumers' personal information

- ❑ Note: Nonprofits are generally exempt, but should still follow privacy best practices and may be subject to other data protection regulations.

Seven Core Privacy Rights

01

Right to Know

Access what personal information is collected, used, shared, or sold

02

Right to Delete

Request deletion of personal information held by businesses

03

Right to Opt-Out

Opt-out of the sale or sharing of personal information

04

Right to Correct

Request correction of inaccurate personal information

05

Right to Limit

Limit use and disclosure of sensitive personal information

06

Right to Non-Discrimination

Equal service and pricing regardless of privacy choices

07

Right to Data Portability

Receive personal information in a portable, usable format

Privacy Policy Requirements

Your privacy policy must be comprehensive, accessible, and updated at least annually. Here's what to include:

Categories of Data Collected

List all personal information categories you collect, including identifiers, commercial information, biometric data, and online activity

Sources and Purposes

Disclose where you obtain personal information and specify business or commercial purposes for collection

Third-Party Sharing

Identify categories of third parties with whom you share personal information and the purposes for sharing

Consumer Rights Procedures

Explain how consumers can exercise their rights with clear submission methods and response timelines

Retention Periods

Describe how long different categories of personal information are retained



Implementing Opt-Out Rights

1 Clear Notice Required

Add a "Do Not Sell or Share My Personal Information" link prominently on your homepage and in your privacy policy

2 Simple Opt-Out Process

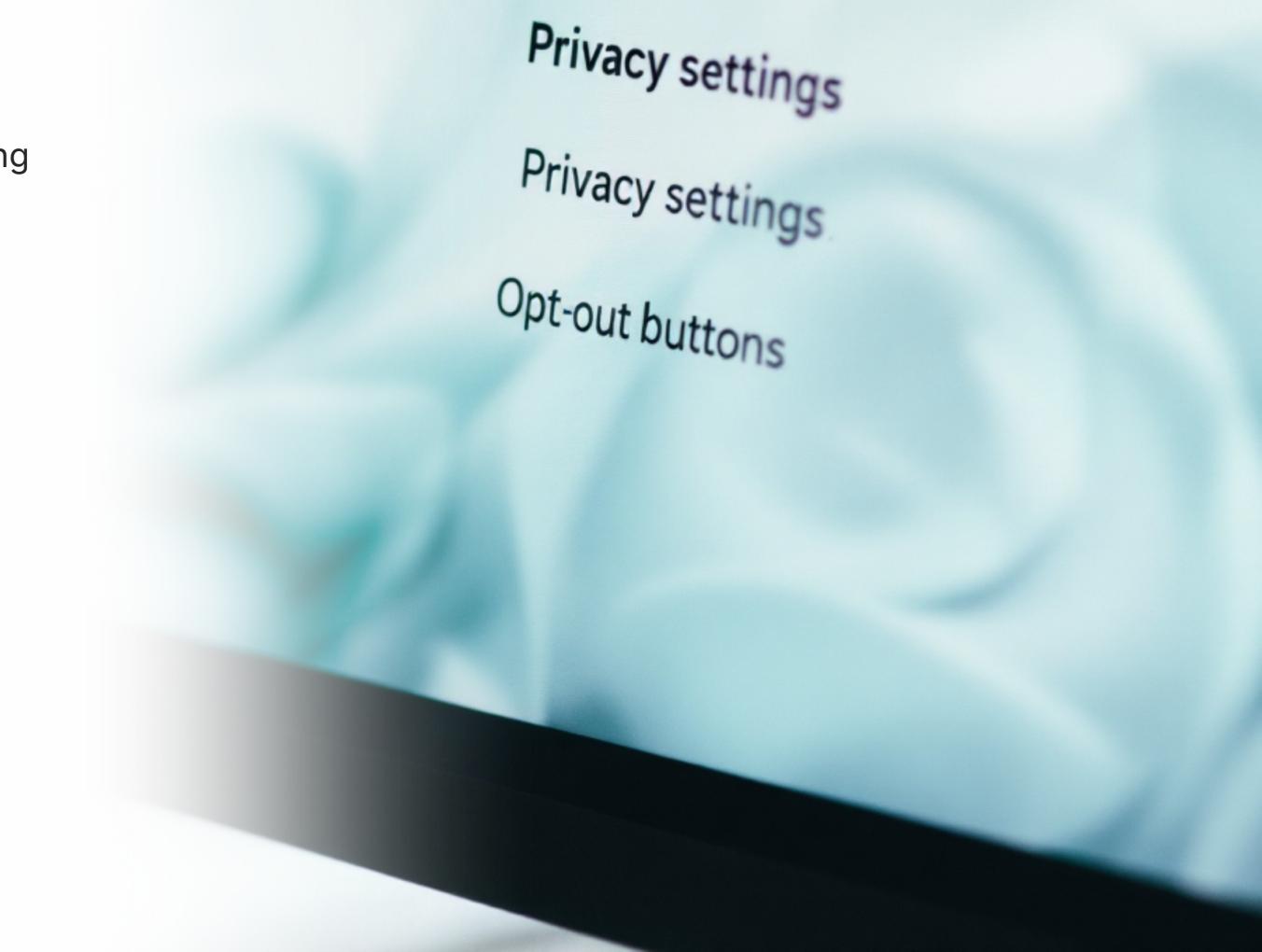
Enable consumers to opt-out through a simple, two-click process without requiring account creation or unnecessary information

3 Honor User-Enabled Signals

Recognize and respond to opt-out preference signals like Global Privacy Control (GPC) automatically

4 No Discrimination Allowed

Maintain equal service quality, pricing, and functionality for users who opt-out of data sales or sharing



Handling Data Subject Requests

Businesses must establish processes to verify and respond to consumer requests within strict timeframes.



Receive Request

Accept requests via toll-free number, website, email, or other designated methods



Search Records

Conduct thorough searches across all systems and databases containing personal information

Verify Identity

Use reasonable methods to verify the consumer's identity without collecting excessive information

Respond Promptly

Provide requested information or complete deletion within 45 days (extendable to 90 days with notice)

Response Timeline

45 days standard response period

+45 days extension available if reasonably necessary

Free of Charge

First two requests per year must be free

May charge reasonable fee for excessive or repetitive requests

Documentation

Maintain records of requests and responses for 24 months

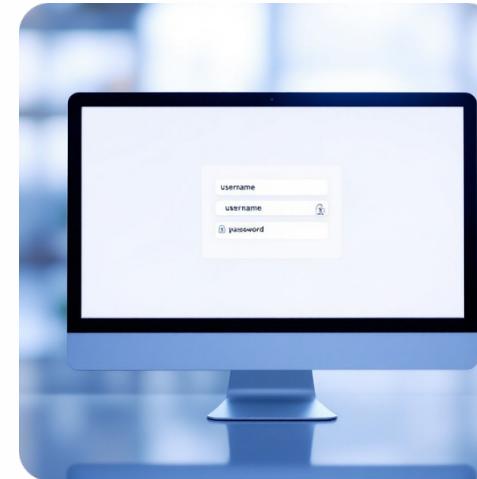
Sensitive Personal Information Protection

CPRA introduces special protections for sensitive personal information, requiring additional consent and limited use.



Identifiers

Social security numbers, driver's license, passport, financial account numbers



Account Access

Usernames and passwords that permit account access



Protected Data

Precise geolocation, racial/ethnic origin, religious beliefs, health data, biometric data, sex life, sexual orientation

- Businesses must provide consumers the right to limit use of sensitive personal information to what's necessary to provide requested services.

Service Provider and Contractor Requirements

When sharing personal information with vendors, businesses must ensure proper contractual protections and oversight.

Written Contracts Required

1

Execute comprehensive agreements with all service providers and contractors who process personal information on your behalf. Contracts must specify permitted uses and require compliance with CCPA/CPRA.

Purpose Limitations

2

Vendors may only use personal information for the specific business purpose outlined in the contract. Prohibit retention, use, or disclosure outside the defined scope.

Certification and Compliance

3

Service providers must certify understanding of data restrictions and implement appropriate technical and organizational measures to protect personal information.

Audit and Monitoring

4

Maintain oversight of vendor compliance through regular audits, security assessments, and breach notification procedures. Document due diligence efforts.

Enforcement and Penalties

The California Privacy Protection Agency (CPPA) enforces CPRA violations with significant penalties. Understanding enforcement mechanisms helps businesses prioritize compliance efforts.

\$2,500 \$7,500 \$750

Per Violation

Civil penalty for unintentional violations

Per Intentional Violation

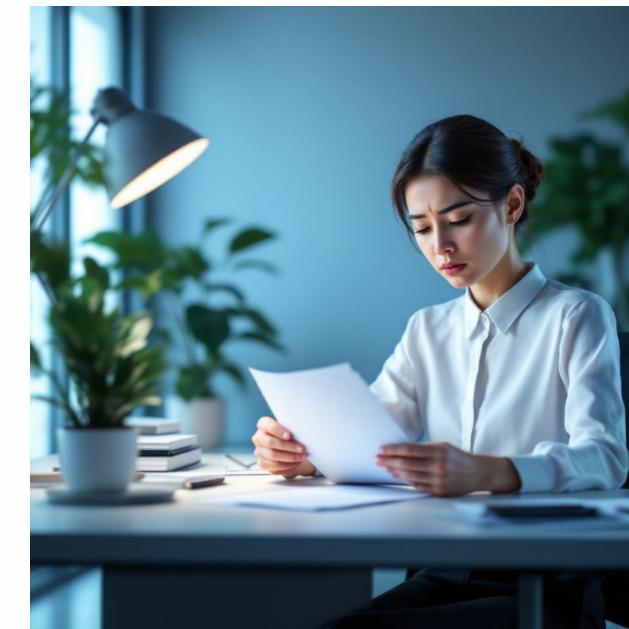
Civil penalty for violations committed with knowledge

Per Consumer

Statutory damages for data breaches (per consumer per incident)

30-Day Cure Period

The CPPA provides businesses a 30-day period to cure violations after notice, though this cure period may be eliminated for certain violations or repeat offenders. Private right of action exists for data breaches involving unencrypted or unredacted personal information.



Key CPRA Enhancements

The California Privacy Rights Act significantly expanded consumer protections and business obligations beyond the original CCPA framework.



New Privacy Rights

Added rights to correct inaccurate data and limit use of sensitive personal information



Extended Lookback

Consumers can request data from previous 12 months (up from 6 months under CCPA)



New Agency

California Privacy Protection Agency established with dedicated enforcement authority



Sharing Restrictions

New "sharing" category covers cross-context behavioral advertising, requiring opt-out options



Risk Assessments

High-risk processing activities now require cybersecurity audits and risk assessments



Employee Data

Expanded coverage to include employee and B2B contact data with full CPRA protections

About Cybersecurity Non-Profit

"Making cybersecurity knowledge accessible to everyone through education, community, and practical resources."

Our Programs

- **Business & Non-Profit Security** – Practical guides for organizations of all sizes
- **Family Cybersecurity** – Protecting your household in the digital age
- **Kids Safety** – Age-appropriate online safety education
- **Senior Digital Safety** – Empowering seniors to navigate technology securely
- **Women's Security** – Privacy and safety resources for women online
- **Parents & Educators** – Tools to teach digital citizenship

Everything we offer is completely free. Visit us at csnp.org to explore our educational resources at csnp.org/resources

Visit CSNP

Browse Resources