



# CCPA & CPRA Endpoint Compliance Checklist

Practical checklist for aligning organizational endpoints with the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) using Codeproof UEM.

*Note: CCPA/CPRA compliance requires policies, data mapping, consumer request workflows, and governance. Codeproof provides endpoint and application safeguards that support these programs; it does not replace legal or privacy counsel.*

## 1) Consumer Rights & Requests (DSARs)

- Support access, deletion, correction, and portability requests by locating device-held data and exporting logs when feasible.
- Use selective wipe to remove business data from BYOD devices during offboarding or upon verified deletion requests.
- Maintain records of requests, response dates, and actions taken (evidence for auditors/regulators).

## 2) Notice, Choice & Opt-Out (Sale/Share, Sensitive PI)

- Ensure apps/browsers on managed devices respect opt-out preferences (e.g., Global Privacy Control) where applicable.
- Restrict ad/analytics identifiers where the platform allows (ad ID limits, tracking controls).
- Configure managed apps to limit use/disclosure of Sensitive Personal Information in line with CPRA requirements.

## 3) Data Minimization & Purpose Limitation

- Allowlist approved apps only; block unapproved or high-risk apps and third-party stores.
- Use containerization (Android Work Profile, Apple User Enrollment) to separate personal and business data on BYOD.
- Apply per-app VPN and data-sharing restrictions to limit exfiltration to authorized services.

## 4) Security of Processing (Reasonable Security)

- Enforce full-disk encryption on laptops and mobile devices (BitLocker/FileVault, OS-native).
- Require strong authentication (passcodes, biometrics, MFA where applicable).
- Encrypt data in transit with TLS/IPSec; disable legacy/insecure protocols.
- Monitor patch posture and quarantine non-compliant devices until remediated.

## 5) Access Control & Accountability

- Apply least-privilege policies; restrict access to personal data to authorized roles only.
- Enforce auto-lock and idle timeout on endpoints with access to personal data.
- Log administrative actions, access attempts, policy changes, and remote actions.

## 6) Vendor & Service Provider Management

- Tag and track contractor/third-party devices; enforce the same controls as employee devices.
- Revoke credentials and selectively wipe business data at contract end or offboarding.
- Keep evidence of configurations pushed to devices that access service-provider environments.

## 7) Audit Evidence & Reporting

- Maintain device and user inventory linked to processing activities where practical.
- Export configuration histories, compliance posture, and incident response logs for assessments.
- Retain records in accordance with retention schedules and regulatory guidance.

## 8) Incident Response & Breach Handling

- Enable remote lock, Lost Mode, selective/full wipe for lost or compromised devices.
- Revoke certificates, tokens, and keys promptly; rotate credentials as needed.
- Document incident timelines and actions taken to support breach notification analysis.

*Copyright © Codeproof Technologies Inc. — This checklist supports CCPA/CPRA alignment on endpoints using Codeproof controls. It is not legal advice.*

---