**1️⃣ Overview**

* **Full Name:** California Consumer Privacy Act of 2018 (amended by California Privacy Rights Act — CPRA, effective Jan 1, 2023).
* **Enforced by:** California Privacy Protection Agency (CPPA) + California Attorney General.
* **Scope:** Applies to **businesses** handling California residents’ personal information, meeting certain thresholds.
* **Goal:** Enhance consumer privacy rights and increase transparency over data collection, use, and sale.

**2️⃣ Applicability Criteria**

CCPA applies if a **for-profit business** does business in California and meets **any** of these:

1. Annual gross revenues over **$25M**, OR
2. Buys/sells/shares **personal information** of 100,000+ consumers or households, OR
3. Derives **50%+ of annual revenue** from selling/sharing consumers’ personal information.

**3️⃣ Key Definitions**

| **Term** | **Meaning** |
| --- | --- |
| **Consumer** | California resident. |
| **Business** | For-profit entity that meets applicability criteria. |
| **Personal Information (PI)** | Any info that identifies, relates to, describes, or could be linked to a consumer/household. |
| **Sensitive Personal Information (SPI)** | SSN, DL number, precise geolocation, financial account info, health data, etc. |
| **Sell** | Selling, renting, releasing, disclosing, disseminating personal info for monetary or other valuable consideration. |
| **Share** | Disclosure for cross-context behavioral advertising. |

**4️⃣ Consumer Rights (Under CPRA)**

| **Right** | **Description** |
| --- | --- |
| **Right to Know** | What PI a business collects, uses, shares, or sells. |
| **Right to Delete** | Request deletion of PI (with certain exceptions). |
| **Right to Correct** | Request correction of inaccurate PI. |
| **Right to Opt-Out** | Stop sale/sharing of PI. Must have “Do Not Sell or Share My Personal Information” link. |
| **Right to Limit Use of SPI** | Limit use of sensitive PI to specific purposes. |
| **Right to Non-Discrimination** | No retaliation for exercising privacy rights. |
| **Right to Data Portability** | Receive PI in a readily usable format to transfer to another entity. |

**5️⃣ Business Obligations**

* **Privacy Notices**: Clearly explain categories of PI collected, purposes, rights, and opt-out mechanisms.
* **Consent Management**: Opt-in for minors (<16), parental consent for <13.
* **Data Inventory & Mapping**: Document all PI categories, sources, purposes, and disclosures.
* **Vendor Contracts**: Contracts with service providers, contractors, third parties to include privacy obligations.
* **Verification Process**: Confirm identity of consumers making requests.
* **Training**: Employees handling PI or consumer requests must be trained on CCPA compliance.
* **Record-Keeping**: Maintain request records for 24 months.

**6️⃣ Enforcement & Penalties**

* **Regulator:** CPPA & California Attorney General.
* **Fine:** $2,500 per violation OR $7,500 for intentional violations / violations involving minors.
* **Private Right of Action**: Consumers can sue for certain data breaches — statutory damages $100–$750 per incident.
* **No Cure Period**: CPRA removed the 30-day cure period for most violations.

**7️⃣ GDPR vs CCPA (High-Level)**

| **Area** | **GDPR** | **CCPA/CPRA** |
| --- | --- | --- |
| Scope | Any personal data of EU residents | PI of California residents |
| Legal Basis | Requires lawful basis (consent, contract, etc.) | Focus on notice & opt-out (consent mainly for minors) |
| Rights | Access, rectify, erase, restrict, portability, object | Know, delete, correct, opt-out, limit SPI use |
| Regulator | Supervisory Authorities in EU | CPPA + Attorney General |
| Penalties | Up to €20M or 4% global turnover | $2,500/$7,500 per violation |
| Breach Notification | 72h to regulator | As per California breach law, private action allowed |
| Data Minimization | Explicit | Implicit (in SPI limitations) |

**8️⃣ Implementation vs Audit Perspective**

**Implementation View**

* Build **data inventory & flow maps**.
* Draft & publish **updated privacy notice**.
* Set up **consumer rights request portal** (online form, toll-free number).
* Implement **verification process** for requests.
* Create **opt-out mechanism** (website link, preference center).
* Review & amend **contracts with vendors**.
* Train employees.

**Audit View**

* Check if privacy notice covers **all required elements**.
* Review request handling logs (response time ≤ 45 days).
* Test opt-out mechanism functionality.
* Verify SPI limitation process.
* Inspect vendor contracts for **CCPA clauses**.
* Confirm training completion for relevant staff.