

## Key Facts

- CCPA effective January 1, 2020.
- CCPA enforced July 1, 2020.
- Privacy rights for California residents.
- Grants new enforcement power to the Attorney General with high damages recoverable.

## 8 Consumer Rights

- Abbreviated Disclosure Right Applicable to Businesses that Collect Personal Information.
- Expanded Disclosure Right Applicable to Businesses that Collect Personal Information.
- Right to Request Information from Businesses that Sell or Disclose Personal Information for a Business Purpose.
- Right to Opt-Out of the Sale of Data.
- Right to Opt-in for Children: Business Obligation Not to Sell Children's Personal Information Without Affirmative Authorization.
- Deletion Rights.
- Rights to Access and Portability.
- Not to be Discriminated Against for Exercising Any of the Consumer's Rights under the Title.

## 8 Business Obligations

- Obligation to Respond to Abbreviated Disclosure Request.
- Obligation to Respond to Expanded Disclosure Request.
- Obligation to Respond to Obtain Opt-In Consent for Children.
- Obligation to Respond to Request for Information from Businesses that Sell or Disclose Personal Information for a Business Purpose.
- Obligation to Respond to Request to Opt-Out of the Sale of Data.
- Obligation to Respond to Deletion Requests.
- Obligations to Respond to Requests for Access and Portability.
- Obligation Not to Discriminate Against Consumers Exercising Their CCPA Rights.

## Key Steps: Action Required

- Establish and communicate responsibility for CCPA compliance.
- Perform a comprehensive and thorough risk assessment, inclusive of a technical cybersecurity assessment.
- Update policies and procedures to address CCPA.
- Remediate gaps for CCPA compliance as identified in the risk assessment.
- Review cybersecurity supply chain (e.g. business associates), including update to contracts/agreements to determine appropriate protection for all California resident data.
- Train members of the workforce to raise higher awareness of CCPA requirements.
- Monitor capabilities implemented actively to ensure appropriate management of controls.

## CCPA Services

- Readiness Assessment:** Identify compliance gaps based on CCPA.
- Cybersecurity Vulnerability Assessment:** Determine security vulnerabilities in the enterprise infrastructure and applications.
- CCPA Policy:** Update policy and align with your compliance and cybersecurity program.
- CCPA Procedure:** Develop tailored CCPA security procedures.
- CCPA Academy:** Acquire CCPA knowledge with the cybersecurity strategy workshop (half-day program, delivered on-site).
- Remediation:** Guidance and support to address CCPA gaps to ensure compliance.
- On-Demand Consulting (ODC) Advisory Services:** Qualified consulting resources and capabilities to assist your efforts to address CCPA.
- Managed Cybersecurity Services Program (MCSP):** Establish and actively manage a CCPA compliance program.
- Cybersecurity Program:** Align CCPA mandates in the context of a broader cybersecurity framework such as the NIST Cybersecurity Framework.

Webinar | On-site Workshop



Talk to ecfirst

Establish a credible  
CCPA compliance program

Perform a CCPA Readiness Assessment.  
Discuss with ecfirst to get started.

## Who Needs to Comply?

- If you are a for-profit business that collects personal information from CA residents and:
  - Annual gross revenue is above **\$25** million.
  - Alone or in combination annually buy, receive, sell or share the personal information of **50,000+** consumers.
  - Derive **50%** or more of its annual revenue from selling consumers' personal information.

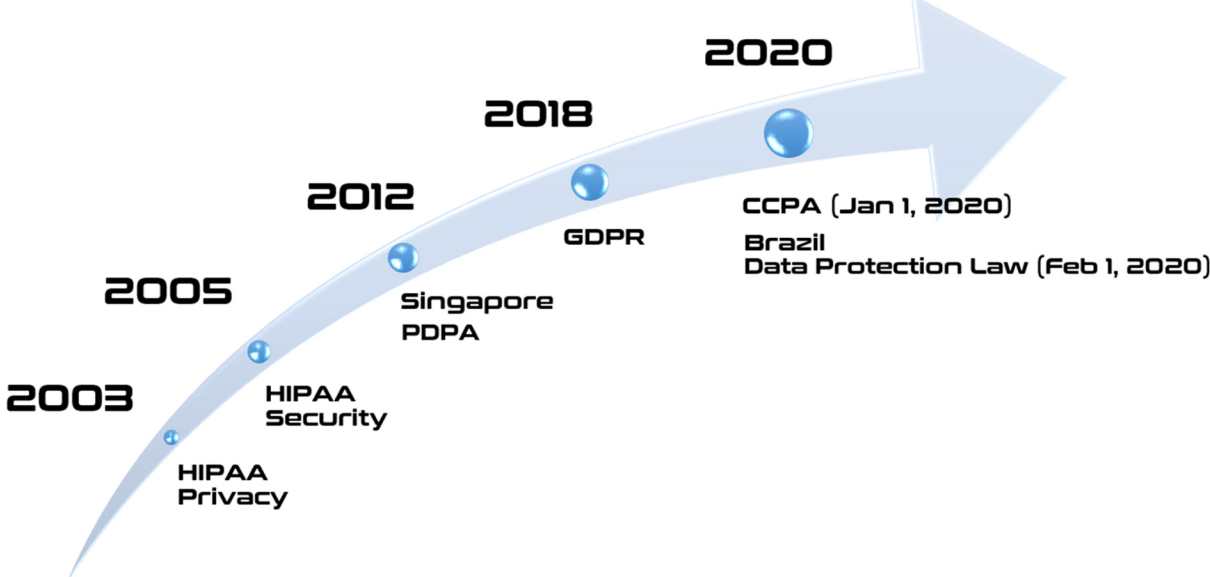
## How Does CCPA Impact Consumers?

Right to Knowledge	Right to be Forgotten	Right to Control Who has Access to their Information
Consumers have the right to request information about: <ul style="list-style-type: none"> <li>What information a company is collecting about them.</li> <li>How that information will be used.</li> <li>If and with whom that information will be shared.</li> </ul>	<ul style="list-style-type: none"> <li>Companies must delete all information they have about a consumer at the consumer's request.</li> <li>Exceptions include:                             <ul style="list-style-type: none"> <li>Data being processed and retained to complete a consumer-requested transaction.</li> <li>Specific research purposes.</li> <li>Limited analytical used other regulatory and contractual exceptions.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Consumers must be able to opt out of the sale of their information to third parties.</li> </ul>

## Penalties

For non-compliance	Unintentional	<b>\$2,500</b>
	Intentional	<b>\$7,500</b>
If personal information is exposed in a data breach	Per incident	<b>\$100–\$750</b> or greater if the actual damages exceed <b>\$750</b>

## The Evolution of Data Privacy Regulations



Protect your rights to tell a business not to share or sell personal information.

## CCPA and GDPR

Factors	CCPA	GDPR
<b>Business scope</b>	Applies to a for-profit "business" that: <ul style="list-style-type: none"> <li>Have USD 25 million or more in revenues.</li> <li>Uses personal data of 50K persons or more for commercial purposes.</li> <li>Derives 50 percent or more from selling personal data.</li> </ul>	Applies to a "controller" or "processor": <ul style="list-style-type: none"> <li>Established in the EU.</li> <li>Established outside of the EU, and either offering goods/services to EU; or monitoring behavior in EU.</li> </ul>
<b>Consumer scope</b>	California residents	EU Data subject – a natural living person in the EU.
<b>Penalty per violation</b>	USD 7,500 per violation for intentional violations	Up to 4 percent global turnover or EU 20 million whichever is higher.
<b>Consumer data request</b>	45 days	30 days
<b>Disclosures</b>	Must disclose information about the collection, sale, and disclosure of personal information in privacy policy or on website. Must provide just-in-time disclosures at or before collection. <b>Opt-out:</b> Don't sell my personal information.	Must provide detailed notice about the collection, use, disclosure of personal data, as well as retention period, individual rights, information about lawful bases for processing, identity of controller/DPO/representative. <b>Opt-in:</b> Consent for certain processing activities.

Perform a risk assessment to identify CCPA gaps and establish a plan for corrective action.

Kris Laidley

Kris.Laidley@ecfirst.com

www.ecfirst.com

Reimagining Cyber Defense

Code: CCPAIG0006