#ForensicPerspectives

CCPA Basics

When?

CCPA went into effect on January 1, 2020.

What is it?

The California Consumer Privacy Act (CCPA) enables Californians to control how companies collect, use, and share their personal details.

Who is protected?

California residents.

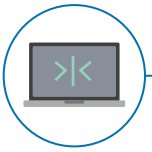
Why act now?

CCPA outlines penalties of up to $2,500 ($7,500 if intentional) per violation, and individuals can seek significant damages following a data breach.

Who must comply?

For-profit companies that work in California and annually earn $25M+, buy/sell the data of 50,000+ people, or earn half their revenue selling personal data.

How is the CCPA different from GDPR?

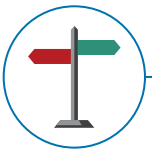


Narrower application

GDPR applies to organizations that maintain an office, offer goods/services, or monitor individuals in the EU. CCPA only applies to certain companies doing business in California.

Limited information

GDPR applies to all personal data. CCPA focuses on non-public data that can be associated with a consumer or a household, such as names, phone numbers, work history, banking details, among others.



Opt-in vs. opt-out

GDPR requires specific, informed, unambiguous, and revocable opt-in consent. CCPA permits California residents to opt-out of storage, sale, and disclosure of their personal information.

"Do not sell my personal information"

CCPA gives California residents the right to opt out of any sale of their personal information. Businesses must include a "Do Not Sell My Personal Information" link on their homepage and/or app.

CRA Charles River Associates

Monitor collection practices for data of children

Business that sell the information of children under 16 must obtain opt-in consent, which can be from the child directly if between 13 and 15 or from the parent if under 13.

Fewer obligations

CCPA does not require companies to: have a legal basis to collect/use personal data, stop transferring personal data outside the US, appoint a data protection officer, or conduct impact assessments.

Right of access

Companies must respond within 45 days to consumers (up to 2x per year) who ask what personal data they collected, where they got it, who it was shared with, and why they collected or sold it.

Portability

While CCPA mandates that a business must give a consumer the option of receiving an access request response in a transmittable format, it does not require the actual transfer as outlined in GDPR.

Class action right

If a California resident's personal data is jeopardized in a data breach, CCPA creates a class action right and an opportunity for statutory damages without a need to demonstrate quantifiable loss.

Penalties

GDPR imposes fines for organizations that fail to properly protect consumer data. CCPA requires a breach and gives companies an opportunity to cure.

Privacy policy

Companies are required to tell consumers what data they are collecting and how it will be used. Certain disclosures are limited to 12 months. GDPR includes no identical obligations or limitations.

Avoid penalties for non-compliance

CRA provides critical expertise in forensic accounting, computer forensics, technology, valuation, and business intelligence. Our Forensic Services team routinely helps companies and their counsel independently respond to allegations of non-compliance. Contact an expert listed below to learn more.

Kristofer Swanson, CPA/CFF, CFE, CAMS
Vice President & Practice Leader, Forensic Services
+1-312-619-3313 | kswanson@crai.com

Josh Hass, CFE, CEDS
Vice President, Forensic Services
+1-212-520-7139 | jhass@crai.com