

A Quick Look at the California Consumer Privacy Act (CCPA)

WHAT

California Consumer Privacy Act (CCPA) is a bill that enhances the privacy rights and consumer protection for consumers and for profit companies that do business in the state of California. It enables consumers to have some control of how a business can store, retain, and use their personal information, and it requires businesses to be transparent in how they are handling consumer data.

WHAT RIGHTS DO RESIDENTS & CONSUMERS HAVE ABOUT THEIR PERSONAL INFORMATION?

To know whether their personal information is sold or disclosed and to whom.

To say no to the sale of personal information.

To access their personal information.

To equal service and price, even if they exercise their privacy rights.

The CCPA sets up a precedent for companies to offer you financial or other benefits for allowing them to sell your data.

WHO DOES THIS APPLY TO?

Applies to any business that houses personal information of California residents which satisfies one or more of the following:

Annual Gross revenue in excess of \$25 million

Alone or in combination, annually buys, receives, sells, or shares for commercial purposes the personal data of 50,000 or more consumers or households

Derives 50 percent or more of its annual revenues from selling consumers personal data

Also applies to an entity that either:

Controls or is controlled by a covered business

Shares common branding with a covered business; name, service mark, or trademark

The CCPA prohibits selling personal information of a consumer under 16 without consent. Children aged 13 – 16 can directly provide consent. Children under 13 require parental consent.

WHEN

CCPA was ratified June 28, 2018 and comes into effect January 1, 2020.

California Consumer Privacy Act (CCPA)

HOW ORGANIZATIONS PROVIDE METHODS TO SUBMIT REQUESTS (minimum of two methods including, at least):

A toll-free number

A web site address (if one is maintained by the business)

HOW ELSE DO ORGANIZATIONS COMPLY TO CCPA? BUSINESSES MUST:

Disclose and deliver requested information for free within 45 days.

Include 12-months worth of data prior to the receipt of the disclosure request.

Deliver the requested information in a readily usable format.

Provide all disclosures related to the collection or sale of personal information and the consumer's rights.

Maintain a list of personal information that is collected AND sold.

Not be obligated to respond to a consumer disclosure request more than twice in a 12-month period.

Provide a clear and conspicuous link on the business's website titled "Do Not Sell My Personal Information."

Consumers shall not be required to make an account with the business to complete this request.

This link must be on the business's homepage, privacy policy, and/or any California-specific privacy page.

Refrain from the sale of personal information for 12 months once a consumer submits a request.

Businesses may choose to have two websites, one for California consumers, and one for others.

Businesses are not required to have this opt-out link available for non-California consumers.

WHY IS THIS CRUCIAL TO UNDERSTAND & IMPLEMENT?

Leverage your data inventory.

Modifications will be necessary to comply with the CCPA.

GDPR's requirements for a "record of processing activities" is far stricter.

Organizations should implement a gap assessment.

This is similar to GDPR assessments.

Determine approach – Apply CCPA rights to all – Limit to Californians?

Determine ability to comply with articles 1798.100-1798.125 (full listing in the law of compliance requirements)

Organizations should re-evaluate a prioritized approach and assess risk.

Remember! Article 1798.150 – How organizations must apply *reasonable* security to consumer data.

Regulators and judges evaluate privacy and data breaches based on an organization's **duty of care**. Organizations must establish their reasonable risk: **DoCRA**.

FINES FOR NON-COMPLIANCE

Provides limited right of action for damages up to **\$750 dollars per person per incident**.

No ceiling for regulatory enforcement, **\$7500 dollars per violation**.