California Consumer Privacy Act (CCPA)

Does CCPA Affect You? What the 2020 Deadline Means

What is the California Consumer Privacy Act (CCPA)?

CCPA is redefining the standard of privacy in the United States. Think of CCPA as GDPR 2.0 – California's own version of the sweeping digital privacy act that was enacted throughout Europe.

CCPA isn't just about California

Yes, this does apply to your business—CCPA isn't just about California! In fact, there's a chance that even though your business doesn't reside in California, this complex compilation of GDPR-like requirements concerning the personal data of California residents will apply to many organizations on **January 1, 2020**. That is when CCPA will become enforceable, and its authority will reach far beyond its borders. Like its European predecessor, GDPR, CCPA is likely to have global applicability. Determining if your company is subject to the rules of CCPA is a simple 2-step process.

First, do you have customers from California or hold the personal data of any California resident?

If YES, then you need to determine if your company meets ANY of these 3 criteria:

- **Has an annual gross revenue in excess of $25 million**
- **Buys, sells or shares the personal information of 50,000+ consumers per year**
- **Derives 50 percent or more of its annual revenues from selling consumers' personal information**

The legislation defines a consumer as a natural resident of the state of California. Considering that California makes up more than 10 percent of the U.S. population, it is likely that companies located throughout the other 49 states will also be affected.

HALOCK®

What CCPA Requires

The purpose of CCPA is to give consumers more rights when it comes to their personal data and to hold businesses accountable for respecting their privacy. The new regulation also aims to bring more transparency about personal data is used and traded amongst companies. Like GDPR, California's new regulation specifically defines what data processing is as it pertains to operations involving personal data. It also sets forth requirements concerning the security and protection of personal data and requires organizations to report data breaches to affected individuals within a defined time window.

CCPA has a broad definition of what constitutes personal data. Under CCPA, personal information includes **any data that can directly or indirectly identify, relate, describe, associate, or link to a particular consumer or household.** Such examples include IP addresses, geolocation data, audio, email address, biometric information, consumer's preferences, psychological trends, bank account number, personal attitudes, and online tracking technologies. CCPA includes a number of requirements such as:

- Default data collection opt-in, ability to opt-out of sale of data, and/or disclosure of data to third parties.
- Opt-out needs to be reaffirmed every 12 months.
- Equal services must be provided or offered, whether residents opt-in or not; companies are able to offer monetary incentives or better services to sell customer data.
- Provides limited right of action for damages up to $750 per person per incident.
- No ceiling for regulatory enforcement.
- Consumers under the age of 16 must affirmatively opt-in in order to allow their personal information to be sold while those under the age of 13 require the consent of a parent or guardian.
- Companies have 45 days to respond to consumer data requests.

Penalties of CCPA

Failure to comply with CCPA regulations will cost you. Once notified of a violation by the Attorney General's office, companies have ***30 days*** to come into compliance in order to avoid. Businesses are subject to civil penalties of up to **$2,500 per violation and $7,500 *per* intentional violation**. A violation could be the compromising of the personal information of a California resident due to a data breach or human error, as well as the selling of one's information without their consent.

FINES FOR NON-COMPLIANCE

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

Civil penalties $2,500 to **$7500 per violation.**

How HALOCK Can Help

Like so many cybersecurity regulations, CCPA repeatedly uses the word "reasonable." The California Attorney General has defined reasonable as the CIS® (Center for Internet Security) controls. HALOCK's team is comprised of experts in compliance regulations, so we can help you determine how the standard applies to your company. HALOCK collaborated with CIS to develop CIS RAM in order to demonstrate how controls are reasonable.

Partnering with Experience

Knowing the type of data that collected, where it is being held, with whom it is being shared, and how it is being transferred is a central component of most data privacy and data security programs. The process of answering these questions is often referred to as a "data inventory." To develop an organization wide privacy program, first, inventory the data that you need to protect, then identify the applicable privacy regulations that need to be addressed. HALOCK can help you through this process.

Privacy regulations typically require a risk assessment to estimate the likelihood and impact of potential harm that may come to individuals due to security and privacy vulnerabilities, and to plan for safeguards that would reasonably address those risks. As principal authors of the CIS® RAM, HALOCK has unique insight of how best to balance compliance, security, and business goals while building **reasonable and appropriate** cybersecurity safeguards by defining your acceptable risk level for your specific environment. Through this approach, your organization can best prioritize and spend your information security dollars while providing a defensable position.

Regardless of what type of business you are, your organization is open to many common attack vectors and errors that compromise security and privacy. For those companies that fall under the jurisdiction of CCPA, the clock is running.

PRIVACY PROCESS MAP (EXAMPLE)

INPUTS

IP address
Device Identifier
Anonymous ID/User ID
Search History
Location data
Usage Statistics
Email address
License plate
Social media information
Phone number
Tokenized CHD+ last 4
Expiration
Name (first/mi/last)
Physical Address
Zip code

INPUT SOURCES

Website
Mobile Applications
Affiliated marketing
Phone

ASSETS

AWS – FS02
Azure
Kubernetes
Mandrill
Legacy AS/400

HOW USED (Sub-Processes)

Guest Purchase
Account Creation
Facility Communications
Tow truck
Monthly parking (need more info)
Looker

3rd PARTIES

AWS
Looker
Optimizely
Salesforce
Segment
Mix panel

CONTROLLERS

ACME
AWS
Azure
Google/Gmail
Salesforce

OUTPUTS

Usage statistics

- Internal reporting
- Marketing tools
- Dashboard

Control Panel

- Reservation times/ durations
- Facility utilization

Internal Reporting

- Sales Statistics
- Demographic reporting for marketing

Partnering with Experience

Knowing the type of data that is collected, where it is being held, with whom it is being shared, and how it is being transferred is a central component of most data privacy and data security programs. The process of answering these questions is often referred to as a "data inventory." To develop an organization-wide privacy program, first, inventory the data that you need to protect, then identify the applicable privacy regulations that need to be addressed. HALOCK can help you through this process.

"HALOCK always met our project goals."

- Energy Company

DATA INVENTORY

Business Process	Sub-Process	Process Owner	SAR Request Contact Details	Asset Name	Description of Controller's Security Controls (Article 32)
ACME Membership	Application-paper form	Membership Director	800.555.1659 SAR@halock.com	Application1	Risk Assessed utilizing controls form CIS v7 & CIS-RAM

Data Categories	Necessary for Business? (Required/ Optional)	Source of Data (Not Provided by Data Subject)	Data Categories	Necessary for Business? (Required/ Optional)
Name (First, Last)	Required	Phone, Fax, Mail	Personal	Required
Middle Name	Optional		Personal	Optional
Former/Maiden Name	Optional		Personal	Optional
Home Address	Required		Personal	Required

Automated Decision Making Y/N	Processor	Description: Processor's Security Controls. (Article 32) [if different than controller]	Processing Beyond Original Intent? (Y/N/ Reason)
No	ACME	Risk Assessed utilizing controls form CIS v7 & CIS-RAM	No

Data Shared with third parties	Data sent outside of EU member states? Where?	Retention Period/explanation for retention (Article 25)	Unstructured data locations (paper/ excel/ etc)
No	No	Retained through membership duration	

HALOCK Security Labs
1834 Walden Office Square, Suite 200
Schaumburg, IL 60173
847-221-0200

Incident Response Hotline: 800-925-0559

www.halock.com

About HALOCK

Founded in 1996, HALOCK Security Labs is a thought-leading information security firm, that combines strengths in strategic management consulting with deep technical expertise. HALOCK's service philosophy is to apply just the right amount of security to protect critical assets, satisfy compliance requirements and achieve corporate goals. HALOCK's services include: Security and Risk Management, Compliance Validation, Penetration Testing, Incident Response Readiness, Security Organization Development, and Security Engineering.