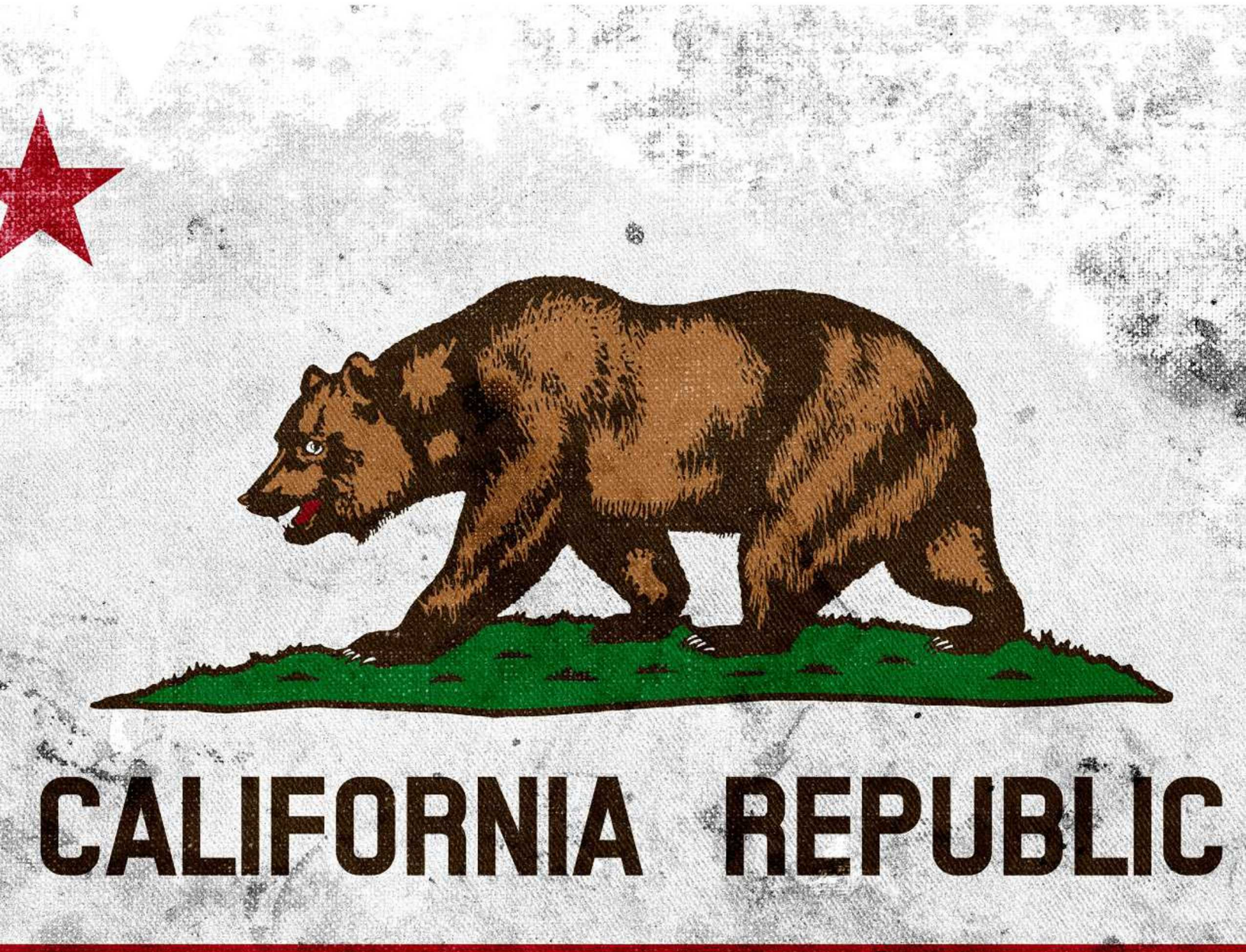
ACA Aponix

California Consumer Privacy Act (CCPA) FAQs



WHAT IS THE CCPA?

The California Consumer Privacy Act (CCPA) allows consumers to find out what personal information of theirs has been collected, to request that companies delete their data, and to opt out of having their information sold. The CCPA requires covered companies to create processes to comply with and facilitate consumer data requests, to update their privacy policies, and to assure that their vendors are in compliance.

Passed as Assembly Bill 375, the CCPA expands on previous California data privacy laws, effectively producing the most comprehensive data use legislation in the United States and granting California residents "increased control" over their data.

WHEN DOES THE CCPA GO INTO EFFECT?

The CCPA goes into effect on January 1, 2020. Enforcement of the law is scheduled to begin on July 1, 2020, or when the California Attorney General completes implementation, whichever comes first.

IS THE CCPA CONTENT FINAL?

While the majority of CCPA content is finalized, several amendments are still under consideration. Some key items under discussion include whether employees will have the same data rights as consumers, whether companies are forbidden to sell consumer reward program information to other companies, whether businesses that operate exclusively online will not be required to provide a toll free number for consumers to initiate requests, whether facial recognition warnings will need to be posted, and more. The changes are working their way through the California Legislature and Governor's office. Any approved amendments need to be signed by the Governor on or before October 13, 2019. At that time we will have the final picture of how the CCPA will be enacted on January 1, 2020 (and we will update this document accordingly).

DOES THE CCPA APPLY TO YOUR FIRM?

The CCPA applies to any for-profit company that:

1. Collects or processes information on California residents, and
2. Meets one or more of the following criteria:

» Has annual gross revenues that exceed $25M
» Derives 50% of revenue from selling consumer data
» Buys, sells, or shares the personal information of 50,000 or more consumers, households, or devices per year

Under these criteria, many companies are implicated by the CCPA. The annual revenue minimum of $25M is applicable to most investment firms or other members of the financial business community. The definition of personal information makes almost any identifying data applicable. The minimum of 50,000 consumers per year criteria makes the law applicable to companies that average 137 credit cards transactions or 137 IP addresses per day, which is more than common for most physical or digital establishments.

WHAT ARE THE REQUIREMENTS OF THE CCPA?

The CCPA enables consumers to control the personal information that companies access and the way it is used. It requires companies to facilitate this control in a clear and specific manner.

While it is advisable to review Assembly Bill 375, the primary requirements of the CCPA include:

» Companies must inform consumers of the general categories and purposes of personal data that will be collected, both at the time of collection and when consumers request it.
» Companies must erase consumer data upon verifiable consumer request (VCR) with exceptions

- (e.g., necessity of the data to complete a transaction, compliance with legal obligations).
- Companies must inform consumers, upon VCR, of the category of third party to which the consumer's data has been sold and the purpose of that sale.
- Companies must facilitate VCRs, including establishing toll-free request lines and prominent website request locations.
- Consumers may opt out of the sale of their personal information. Companies that sell consumer data must provide prominent "Do Not Sell My Personal
- Information" web notifications and opt-out mechanisms. Companies should not prompt consumers to change their data privacy preference for 12 months after the consumer selects their preference.
- Companies may not sell the personal information of minors without obtaining opt-in from parents or guardians.
- Companies must clearly display their privacy policy for consumers, including notification of consumer data rights.
- Companies may not discriminate against consumers based on their data privacy requests.

WHAT ARE THE CCPA'S REQUIREMENTS REGARDING VENDORS?

Upon request, companies are required to disclose the sale of consumer data to third-party vendors. Third-party vendors may not resell consumer data unless consumers have received explicit notice and have been given the opportunity to opt out.

In general, companies must ensure that the third-party vendors they work with are in compliance with the CCPA. Partners and vendors must be carefully vetted prior to and during engagements. Parties will need to be clear about the data they are collecting, sharing, and selling, and must include protections in their contracts regarding regulatory enforcement or consumer class actions.

WHAT DATA IS COVERED BY THE CCPA?

The CCPA's definition of consumer personal information is broad and inclusive.

Personal information is defined as any "information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household." This expansive definition goes beyond obvious data (e.g., names, addresses, credit card numbers, social security numbers) to include device geolocation data (e.g., IP addresses), biometric information (e.g., fingerprints, retina scans, height, weight, medical data), or even gender or zip code. It applies to any household, including those of consumers or employees.

WHAT ARE THE PENALTIES FOR NON-COMPLIANCE WITH THE CCPA?

The fine per civil violation is $2,500 to $7,500 for each violated data record, with the fine of $7,500 reserved for intentional acts of CCPA non-conformity. Companies have a 30-day cure period following notification.

HOW ARE DATA BREACHES HANDLED UNDER THE CCPA?

The CCPA requires companies to "implement and maintain reasonable security procedures and practices" to safeguard consumer data.

While penalties for general CCPA non-compliance are enforced by the California Attorney General's office, data breaches fall in a different category. If a breach occurs, and the covered company is deemed to have not implemented appropriate security procedures, consumers can take a "private cause of action" against the company. After a 30-day cure period, consumers can demand statutory damages within a range of $100-$750 per consumer per incident. Consumers can likewise demand actual out-of-pocket damages, without a notification period.

ARE THERE ANY EXCEPTIONS TO THE CCPA?

There are certain exceptions to CCPA restrictions regarding the collection and usage of consumer data. Some important types of data that are not in scope of the CCPA include:

- Public information that is not considered personal information
- De-identified or aggregated data that is not considered personal information
- Data from consumers who are not residents of California
- Data utilized to comply with local, state, and/or federal laws (i.e., HIPAA, GLBA)
- Data utilized to cooperate with law enforcement
- Data in mergers and acquisitions, bankruptcy, or other corporate transactions, in which the acquiring entity protects the data from unlawful sale or usage

HOW DOES THE CCPA COMPARE TO THE GDPR?

- Both the CCPA and the European Union's General
- Data Protection Regulation (GDPR) are broad pieces of legislation that are related to consumer data privacy. However, expansion of GDPR compliance measures to include California residents does not automatically imply compliance with the CCPA.
- The CCPA differs from the GDPR in the following ways:
- The CCPA demands several concrete request, disclosure, and notification mechanisms not included in the GDPR, including toll-free phone numbers, prominent online opt-out mechanisms, expanded privacy notices, etc.
- The CCPA and the GDPR have nuanced differences in their definitions of personal data (e.g., the CCPA includes "household data" in a slightly different context). Close study of CCPA requirements, or a "highest common denominator" approach between the legislation, is warranted.
- The CCPA provides specific and narrow definitions of entities the law applies to, which differs from the GDPR. For example, under the CCPA, "processors" are not directly liable.
- The scope and methods of disclosure required by the GDPR are somewhat greater than those required by the CCPA. While both regulations have similar disclosure requirements, there are some subtle differences. For example, the CCPA requires only a 12-month timeframe, while the GDPR does not have this limitation. Similarly, rules for data portability are slightly different.
- The CCPA and GDPR have differences in deletion rights. CCPA deletion rights apply only to data collected from the consumer, not from third parties about the consumer. The CCPA further provides a greater number of exceptions to data deletion rights (e.g., contracts, free speech issues, government investigations).
- The CCPA and GDPR have differences in opt-out rights. Close study, or a "greatest highest denominator approach" would be needed to ensure compliance with both regulations.

In general, it is advisable for companies to treat the GDPR and the CCPA as separate sets of regulations that are part of a larger, holistic strategy for data privacy compliance.

HOW CAN MY COMPANY ENSURE COMPLIANCE WITH THE CCPA?

Companies need to take steps to meet the regulation's requirements before CCPA takes effect on January 1, 2020.

In addition to monitoring for any additional amendments that may add, change, or remove CCPA compliance requirements, here are five steps your company should take to prepare for the compliance deadline:

- Obtain executive buy-in – CCPA compliance is a broad effort that will affect many aspects of your company and will require significant staff hours and financial resources. In addition, failure

to comply can have serious financial and reputational consequences. As a result, it is crucial to gain executive buy-in to facilitate the compliance process.

- Understand your data collection policies and procedures – It is essential to understand what your company's current policies and procedures are for collecting, storing, and selling data on California consumers. Prepare data maps, inventories, and other records that clearly illustrate what data your company collects and sells, and where it is sold.
- Prepare a gap analysis – Review CCPA requirements closely and compare them with your data discovery findings. Perform a detailed delta assessment between your company's current status and where it needs to be for compliance.
- Develop a compliance roadmap – Develop a comprehensive compliance roadmap of necessary action steps based on the results of the gap analysis. Prioritize tasks based on risk and level of effort.
- Implement the compliance roadmap – Assign leaders for the remediation effort, and delegate tasks to responsible parties. Follow up on progress regularly. Develop all necessary updates and mechanisms (e.g., privacy policies, opt-out, opt-in, web updates, etc.). Test and fix all solutions as necessary. Update due diligence policies regarding third-party vendors and vet vendors for compliance as well. Include staff training as part of the overall compliance effort.

HOW ACA APONIX CAN HELP

ACA's CCPA compliance assistance service is designed to assess your company's readiness to comply with CCPA requirements and to help implement best practices for achieving broader privacy risk and compliance objectives across your enterprise. Our team of experienced consultants can review your company's personal data collection activities, build a data inventory, identify risks and gaps relative to the requirements of CCPA, and assist with building a practical action plan to address deficiencies.

We welcome the opportunity to speak to you.

For more information on ACA Aponix and our services, please contact:
sales@acaaponix.com | +1 (646) 531-5750