Comprehensive FAQs on the CCPA

Insights
5.24.23

The California Consumer Privacy Act (CCPA) has created compliance challenges across the country for businesses – but they often stem from the fact that businesses are confused about some of the law's basic principles. This series of Frequently Asked Questions, prepared by the Fisher Phillips' Consumer Privacy Team, offers a thorough interview to help not only those brand-new with the law but also those well-versed and experienced in compliance efforts.

What is the difference between the CCPA and the CPRA?

The CCPA, or California Consumer Privacy Act of 2018, was passed in 2018. The CPRA, or California Privacy Rights Act of 2020, amended the CCPA. The CPRA took effect in phases, with all remaining sections taking effect January 1, 2023. The CPRA is not a separate law; it is just an amendment to the CCPA passed by the voters in the November 2020 election (Proposition 24).

Who is a consumer?

Despite the word choice, the CCPA and CPRA are not limited to just transactional customers of a business, as in end-users or members of the public who directly purchase goods or services. A consumer for purposes of the CCPA/CPRA is any natural person who is a California resident. This includes any of the following if they are a California resident:

- job applicants
- current and former employees
- emergency contacts, family members, dependents, and beneficiaries of employees
- temporary works on assignment through a staffing agency
- individuals providing services as independent contractors
- employees, owners, directors, officers, and independent contractors of any entity with which your business interacts in any capacity, including other companies, vendors, suppliers, auditors, nonprofits, government agencies, and professional service providers
- members (if your business is membership based)
- visitors and guests to your office, facility, store or other physical location in California
- website or app users

Physical presence in California does not automatically qualify the consumer as a resident of the state, and the law does not create a presumption of residence status based solely on the interaction taking place in California. There are several tests for residence status under this law, of which the most common tests are

primary residence, domicile, or having spent more than 6 months out of the last 12 months in California even if the person's primary resident or domicile is in another state.

Is my business subject to the CCPA?

As of January 1, 2023, the CCPA applies to any business that (a) "does business" in California, (b) operates for the profit *or* financial benefit of its shareholders or owners, (c) collects personal information from one or more California residents (including even a single employee or customer), and (d) satisfies at least one of the following thresholds, is subject to the CCPA:

- Has gross annual revenue in excess of $25 million in the preceding calendar year (measured on January 1 of the calendar year)
- Annually buys, sells, or shares the personal information of 100,000 California consumers or households
- Derives 50% or more of its annual revenue from selling or sharing personal information

Another way your business could be subject to the law relates to whether your business controls or is controlled by a CCPA-covered business while also sharing common branding and sharing personal information. Or you could operate a joint venture or partnership comprised of covered businesses in which any covered business has at least a 40% interest. Or you could voluntarily certify to the California Privacy Protection Agency that you are in compliance with and agree to be bound by the CCPA.

You can dive deeper into this subject by reviewing our helpful summary, Does the CCPA Apply to Your Business?

Note: the CCPA generally does not apply to nonprofit organizations (unless sharing the branding of a covered business, or unless the nonprofit is entirely member-owned and provides goods or services for the financial benefit its members/owners), or to government agencies. However, there is a critical difference between "nonprofit" and "not-for-profit" institutions, the latter of which may operate for the "financial benefit of its shareholders or other owners."

Is my business subject to the CCPA even if my business is based outside of California?

Potentially, yes, if you meet one of the four tests under the CCPA. The CCPA applies to businesses that do business in California, even if not organized under California law and even with no physical presence in California.

What does it mean to "do business" in California?

Unfortunately, the CCPA and the CPRA do not specify what this critical phrase means. A company might be considered to "do business" in California even if it merely operates a website or app through which California residents are allowed to provide their personal information.

The CCPA carves out a narrow exception if every aspect of commercial conduct takes place wholly outside of California. What that means is:

- The business collects personal information of California residents while they are outside of California;
- No sale of the California resident's personal information occurs in California; and

- No personal information collected while the California resident was in California is sold.

The following is a non-exhaustive list of what may potentially constitute doing business in the State of California:

_____ Engagement in any transaction for the purpose of financial gain within the state

_____ Domiciled in or maintains a physical location

_____ Has one or more employees or independent contractors located in the state

_____ Recruits potential job applicants from within the state

_____ Markets or sells its products or services in the state

Is the revenue threshold just for revenue generated in California?

No. The revenue threshold is established by gross revenue regardless of source, location of where the revenue is generated, or any other factor. Thus, all gross revenue from anywhere in the world should count towards the threshold, not just California revenue.

Over what period is revenue measured?

As of January 1, 2023, the calculation is based on all revenue generated during the prior calendar year (that is, from January 1 through December 31). That means that as of January 1 in any given year, if the business did not meet the revenue threshold in the prior calendar year, then the next time the CCPA may begin to apply to the business is the following January 1.

Will collecting data through our website count towards the "buy, sell, or share" criteria?

Under the prior version of the CCPA (effective January 1, 2020 through December 31, 2022), yes. Collection of a California resident's data through a website satisfied the initial requirement for CCPA coverage. This included IP addresses and other internet activity information such as device ID, browser ID, what the user clicked on, etc. Under the prior criteria, data collected through a website could qualify as "personal information" of a California resident even if the business did not actually collect the person's name and contact information, so long as the data collected could reasonably be used (by the business or by any third party with whom the data can be shared) to identify or link to the individual consumer.

Accordingly, the second criteria under the prior test for CCPA applicability was met if your website collected on an annual basis personal information from over 50,000 California residents, households, or devices.

However, starting on January 1, 2023, your website will continue to meet the second criteria only if the collection includes the buying, selling or sharing of personal information from over 100,000 California residents or households on an annual basis. Selling and sharing have special meanings under the CCPA, and

they can potentially include analytics and use of personal information for targeted advertising to your website users on third-party websites and social media.

As a result of the change in the law that took effect January 1, 2023, data about/from "devices" will no longer be part of this criteria, but it is yet to be seen whether the removal of this term from the criteria will be interpreted to mean that collection of data about website visitors through cookies and pixels and then sharing or selling this data would bring a business within the scope of this criteria.

If we operate a franchisee, subsidiary, or parent company, how do we know if the CCPA applies to us?

Even if you are not a covered business, as discussed above, entities that control *or* are controlled by a covered business, along with those that share common branding with a covered business (such as a shared name, servicemark, or trademark that the average consumer would understand that two or more entities are commonly owned) are covered by the law. In such cases, your business is not exempt from CCPA coverage merely by being a franchisee or subsidiary.

Starting in 2023, however, this additional test will only apply if there is also the sharing of California residents' personal information. To be clear, the test now has three parts: (1) control; (2) common branding; and (3) sharing of personal information.

Control can be established in any of the following ways:

- ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting security of a business;
- control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or
- the power to exercise a controlling influence over the management of a company.

How long do I have to comply with the CCPA?

The CCPA went into effect on January 1, 2020, so you should already be compliant with the pre-2023 provisions of the law, including the CCPA regulations that took effect in August 2020.

In November 2020, California voters approved the CPRA to expand the reach of and not replace the CCPA. As such, the CCPA requirements that are unchanged by the CPRA remain in effect after the CPRA is implemented.

January 1, 2023 was the deadline to comply with the CPRA statutory changes that took effect on that date.

March 29, 2023 was the deadline to comply with new CCPA regulations that were implemented by the newly established California Privacy Protection Agency (CPPA).

When will California begin enforcing CCPA requirements?

CCPA regulations and requirements have been and continue to be enforced by the California Attorney General since July 1, 2020.

Starting July 1, 2023, the California Privacy Protection Agency (CPPA) will share authority with the California Attorney General to enforce the CCPA (including the statutory requirements that took effect January 1, 2023, and the new regulations that took effect March 29, 2023) against non-compliant businesses. The CPPA will have broad authority to investigate and audit businesses.

In addition, as of January 1, 2023, the CPRA eliminated the mandatory "cure provision" that previously provided businesses a 30-day period to bring themselves into compliance without being subject to penalties.

What are the consequences for non-compliance? Are there enforcement penalties?

Any business that violates a provision of the CCPA or CPRA may be liable for a civil penalty up to $2,500 for each violation or $7,500 for each *intentional* violation. Civil penalties can only be imposed in enforcement actions by the Attorney General or the California Privacy Protection Agency.

Under the CCPA, the consequences for a data breach involving certain sensitive personal information are severe. This is in large part due to the CCPA's "private right of action" allowing California residents who prove a violation to recover statutory damages between $100 and $750 *per person*, *per incident*, even if the person cannot prove actual harm. These penalties can add up quickly, particularly in a class action context. Your defense against any statutory damages is being able to demonstrate that you implemented and maintained reasonable security procedures and practices.

What is the significance of the CCPA "private right of action"?

Under the CCPA, individuals have a "private right of action" against a business if certain categories of their nonencrypted and unredacted sensitive personal information was stolen in a data breach resulting from the business's failure to maintain reasonable security procedures and practices.

Currently, the CCPA limits a data breach to only unauthorized access and exfiltration, theft, or disclosure of an individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

- Social security number
- Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
- Medical information
- Health insurance information
- Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes
- Genetic data

The CPRA, effective January 1, 2023, expanded the scope of privately enforceable violations to include email addresses in combination with a password or security question and answer that would permit access to the California resident's account.

Do we qualify for any CCPA exemptions?

The CCPA does not have entity-level exemptions. It is possible that some types of data used for particular purposes may be exempt, but the law does not blanketly carve out certain businesses or types of businesses. If one of the tests applies to you, the CCPA applies to your business.

For example, data that is entirely subject to the Gramm-Leach-Bliley Act (GLBA) is not subject to the CCPA so long as it is collected, processed, sold, or disclosed for a GLBA-covered purpose, meaning for the purpose of providing a financial product or service by a financial institution. If the same data is used for marketing purposes not covered by GLBA, then the use of the data for such purpose would still be subject to the CCPA.

Similarly, a HIPAA-covered entity is not automatically exempt from the CCPA. Only the data may be subject to the HIPAA exemption from the CCPA and only to the extent the data itself qualifies as protected health information (PHI) and is used for HIPAA-covered purposes. If data that is not PHI is shared with a HIPAA-covered entity, the HIPAA-covered entity and the business's sharing of such non-PHI data with such HIPAA-covered entity would still be subject to the CCPA.

What are the current training requirements under the CCPA?

Under current law, covered businesses must ensure that all individuals responsible for CCPA compliance or handling responses to consumer inquiries are informed of CCPA requirements. This includes knowing how to direct consumers to exercise their rights under the CCPA.

The CCPA regulations contain a similar training obligation, but in addition require businesses to establish, document, and comply with a training policy if they know, or reasonably should know, that they buy, receive, sell, or share, for commercial purposes, the personal information of 10 million or more consumers in a calendar year.

Did the CCPA training requirements change when the CPRA took effect?

No. The training requirements remain the same.

Who should we train?

Compliance requires employers to ensure that any employee involved in implementing, managing, or overseeing compliance with the CCPA receives training. This includes executives, general managers, human resources employees, directors of marketing, social media managers, and information technology employees. Additionally, any employee responsible for handling consumer requests through the business's CCPA toll-free hotline must receive the training.

Finally, you should train employees who regularly interface with consumers – such as sales representatives – on the basic requirements of the CCPA and where to direct consumer questions and requests regarding data privacy.

What must the training cover?

Employees must understand their role in CCPA compliance. This includes understanding that employees *and* job applicants are "consumers" under the law and have the same rights, including the right to be free of retaliation from exercising their CCPA rights.

Training must cover consumer rights created under the CCPA. Specifically, training should cover the consumer's individual right to request any of the following:

- Copies or deletion of specific personal information collected;
- Disclosure of the categories of personal information collected, the source(s) from which the information was collected, the business purpose for collecting or selling that information, *and* the categories of third parties with which that information was shared up to 12 months prior;
- For businesses selling or disclosing their personal information for any business purpose, disclosure of the categories of personal information collected, sold, or disclosed;
- Limiting the use or disclosure of "sensitive personal information" (a sub-category of personal information); and
- Corrections to personal information.

Training should also encompass the following:

- A consumer's right to not be discriminated against for exercising any right under the CCPA;
- How businesses should inform consumers of their rights under the CCPA;
- CCPA requirements for offering financial incentives to consumers in exchange for the collection of their personal information; and
- Methods for delivering requested information to a consumer after receiving a consumer's request.

How long must the training be?

The law does not specify. Practically, however, the training for managerial employees may take up to two hours in length or more, as it should cover all aspects of compliance with the CCPA.

Training for non-managerial, consumer-facing employees may be shorter and cover the main provisions of the CCPA based on the employees' level of involvement with compliance. For example, they may need to know about the specific forms and notices they may need to give consumers.

Who can provide the training?

The law does not require any minimum qualifications for those who provide training. However, as the CCPA is highly technical, we recommend that someone with data privacy experience provide the training. Members of the Fisher Phillips Consumer Privacy Team have been providing this training for employers and can do so across all industries.

How often is the training required?

The law does not specify how often employers must provide training. New regulations may provide additional guidance in the future, but for now we recommend that employees receive a refresh on CCPA compliance on an annual basis.

Will businesses face penalties for failing to provide training?

In the context of training, it is yet to be determined whether the penalty would be established on a "per employee basis" (for each employee who did not receive adequate training) or counted as single violation for not providing adequate training to all persons required. Therefore, it is important to comply with your training obligation and document employees' attendance at all training events to establish a record of compliance.

Conclusion

Fisher Phillips will continue to monitor CCPA obligations and enforcement efforts and provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insights to get the most up-to-date information direct to your inbox. For further information, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on the firm's Consumer Privacy Team.

Related People

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Darcey M. Groden, CIPP/US
Associate
858.597.9627
Email

Anne Yarovoy Khan
Of Counsel
949.798.2162
Email

Jenna Rogenski
Associate
415.490.9013
Email

Christopher M. Champine
Associate
858.597.0278
Email

Anthony Isola
Partner
415.490.9018
Email

Benjamin M. Ebbink
Partner
916.210.0400
Email

Service Focus

Data Security and Workplace Privacy

Consumer Privacy Team

Emerging Issue Focus

CCPA Resource Center

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills