Published on *The National Law Review* https://www.natlawreview.com

# California Consumer Privacy Act FAQs for Covered Businesses October 2019

Article By:

Joseph J. Lazzarotti

Jason C. Gavejian

Set to take effect January 1, 2020, the **California Consumer Privacy Act (CCPA)**, considered one of the most expansive U.S. privacy laws to date, places limitations on the collection and sale of a consumer's personal information and provides consumers certain rights with respect to their personal information.

Organizations should be doing their best to determine if they have CCPA obligations directly as a business, because they control or are controlled by a business, or because they have contractual obligations flowing from a business.

These FAQs should help businesses determine whether they are indeed subject to the CCPA, and, if so, learn more about the CCPA's obligations and how to implement policies and procedures to ensure compliance.

## 1. Which businesses does the CCPA apply to?

In general, the CCPA applies to a "business" that:

A. Does business in the State of California;

B. Collects personal information (or on behalf of which such information is collected);

C. Alone or jointly with others determines the purposes or means of processing of that data; *and*

D. Satisfies at least one of the following:

1. Annual gross revenue in excess of $25 million;

2. Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of at least 50,000 consumers, households, or devices; or

3. Derives at least 50 percent of its annual revenues from selling consumers' personal information.

***"Annual Gross Revenue" and "50,000 or more consumers."*** Some of the thresholds for determining whether a business is covered by the CCPA remain unclear. For example, it is still unclear whether annual gross revenue is to be measured globally or only from California sources. In the case of the threshold for collecting personal information of at least 50,000 consumers each year, many businesses may not realize how easily this number could be reached. One reason is these businesses are not yet familiar with how broadly "personal information" is defined (see below). Attorney General regulations may help to clarify these and other remaining questions about the application of some of the law's key provisions.

***Related entities and not-for-profits.*** Under the CCPA, a "business" can be a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners." Thus, for example, a business under this definition generally would not include a not-for-profit or governmental entity. It also would not include a corporation that meets the first three criteria above, but not the fourth.

However, a "business" under CCPA also includes any entity that controls or is controlled by a business that meets the requirements above and that shares common branding with such a business. "Control," for this purpose, means:

1. Ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business;

2. Control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or

3. The power to exercise a controlling influence over the management of a company.

"Common branding" means a shared name, servicemark, or trademark. Accordingly, organizations that would not themselves be a "business" under the CCPA could become subject to the law because of the entities that control them or that they control and with which they share common branding.

***Businesses that do not collect consumer personal information.*** A business may not need to actually collect personal information from consumers to be covered by the law. If personal information is collected on behalf of a business (such as through a third-party service provider), the business could be covered by the CCPA as long as the other criteria are satisfied.

Some businesses believe that, because they do not transact directly with individual consumers (as traditional "consumers" or individuals purchasing goods or services for their personal, family, or household use) and collect personal information, they are not subject to the law. That the businesses' "consumers" are other businesses and not individuals make no difference under the CCPA. A consumer under the CCPA's original language is defined broadly and generally to mean a natural person who is a California resident. Accordingly, when conducting business with other businesses, a business likely collects personal information from contacts at the other businesses. Similarly, virtually all businesses collect information about their employees. Recent legislative activity

provides some exceptions to address these categories of business contacts and employees (more on this below).

***Businesses located outside of California — the "long arm" of the CCPA.*** A business may not need to be located in California to be subject to the CCPA. While the CCPA does not expressly address this, a business may be "doing business" in California if it conducts online transactions with persons who reside in California, has employees working in California, or has certain other connections to the state, even if there is no physical location in the state. Regulations from the Attorney General may help to clarify what "doing business in California" means for purposes of the CCPA.

***Businesses that process information on behalf of other businesses.*** The definition of a business under the CCPA requires that the business, alone or jointly with others, "determine[s] the purposes or means of processing" of personal information. The CCPA gives no additional guidance on this language. However, as the nearly identical language is used in the General Data Protection Regulation (GDPR) to define a controller (the term equivalent to "business" under the CCPA), guidance from the UK's Information Commissioner may provide some insight.

Factors that may help to determine if a business is a controller:

- The business decides to collect or process the personal data.
- The business decides what the purpose or outcome of the processing is to be.
- The business decides what personal data should be collected.
- The business decides which individuals to collect personal data about.
- The business obtains a commercial gain or other benefit from the processing, except for any payment for services from another controller.
- The business processes the personal data as a result of a contract between the business and the data subject.
- The business exercises professional judgment in the processing of the personal data.
- The business has a direct relationship with the data subjects.

An organization that merely processes personal information for businesses covered by the CCPA might argue it is not directly subject to the CCPA. It may be correct, but if it has business partners that are subject to the CCPA, it may acquire by contract CCPA obligations from its business partners.

## 2. What is personal information under the CCPA?

In general, the CCPA defines personal information broadly to include information that can identify, relate to, describe, be associated with, or be reasonably capable of being associated with a particular consumer or household. Significantly, the CCPA's private right of action provision relating to data breaches incorporates a narrower definition of personal information (more on this below).

The statute provides a non-exhaustive list of categories of personal information, including:

- Identifiers including real name, alias, postal address, unique personal identifier, online identifier, internet protocol (IP) address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
- Characteristics of protected classifications under California or federal law;
- Commercial information, including records of personal property, products, or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- Biometric information;
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement;
- Geolocation data;
- Audio, electronic, visual, thermal, olfactory, or similar information;
- Professional or employment-related information; and
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (FERPA).

The definition also pulls in inferences from personal information used to create a profile about a consumer that would reflect the person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. Thus, for example, businesses that leverage artificial intelligence (AI) to help determine consumer preferences or identify preferred job candidates must look more carefully at what personal information they may maintain about their consumers (including employees) for purposes of CCPA.

Personal information does not include de-identified or aggregate consumer information.

## 3. What rights do consumers have over their personal information under the CCPA?

Covered businesses have an obligation to develop programs to manage the sweeping suite of rights the CCPA grants to consumers. Below is a rundown of CCPA consumer rights:

***Notice.*** A business that collects a consumer's personal information must inform consumers, at or before the point of collection, as to the categories of personal information to be collected and the purposes for which the categories of personal information will be used. This does not include specific pieces of personal information.

In addition, covered businesses must disclose certain information in an online privacy policy or on an internet website, as applicable. This information includes, without limitation, an explanation of the

rights consumers have under the CCPA (see below) and certain information about the categories of personal information it collected, disclosed, or sold, as applicable. These disclosures must be updated every 12 months.

***Access & Information.*** The CCPA grants consumers the right to request information regarding:

- The categories of personal information businesses collect about them (*e.g.,* identifiers such as their names, Social Security numbers, IP addresses, email addresses, postal addresses; commercial information such as purchasing histories; geolocation data, biometric information, internet activity such as web browsing histories; and professional or employment-related information);

- The sources from which that personal information was collected (*e.g.,* online order histories, online surveys, marketing companies, tracking pixels, cookies, web beacons, or recruiters);

- The categories of personal information sold to third parties;

- The categories of personal information disclosed for business purposes;

- The categories of third parties to whom personal information was sold or disclosed (*e.g.,* tailored advertising partners, affiliates, social media websites, service providers);

- The business or commercial purposes for which personal information was collected or sold (*e.g.,* fraud prevention, marketing, improving customer experience); and

- The "specific pieces" of personal information collected.

The CCPA imposes a 12-month lookback from the time of the request and mandates that, if consumers request access to their personal information, the covered business provide responsive materials "in a readily usable format that allows consumers to transmit [the] information from one entity to another without hindrance."

***Deletion.*** With some exceptions, the CCPA permits consumers to request that covered businesses, and their direct service providers, to delete personal information collected about them. Deletion is not required if the covered business needs the personal information to complete the transaction for which it was collected; to comply with a legal obligation, such as a record retention requirement; to protect against malicious, deceptive, fraudulent, or illegal activity; or to identify and repair errors that impair existing and intended functionality.

***Opt Out.*** Under the CCPA, consumers are empowered to opt out of the "sale" of their personal information. To facilitate consumers' exercise of this right, covered businesses must provide a "Do Not Sell My Personal Information" link on the business's internet homepage to a web page where consumers can opt out of having their personal information sold to third parties.

***Nondiscrimination.*** The CCPA prohibits covered businesses from discriminating against consumers for exercising their CCPA rights. For example, a business may not charge a different price, deny goods or services, or impose penalties on a consumer who exercises his or her rights under the CCPA. However, a business may charge consumers a different price or rate or provide a different level or quality of goods or services to the consumer when that difference is reasonably related to the

value provided to the business by the consumer's data.

## 4. Can consumers waive their rights?

No. The CCPA expressly prohibits any contractual provision or agreement that attempts to waive or limit rights provided by the CCPA, including the right to remedy or enforcement. Accordingly, any attempt to limit a consumer's rights, whether by contract, agreement, or policy, would be unenforceable.

## 5. Does the CCPA apply to employee data?

Employee personal information has been a highly contested matter throughout the CCPA's amendment process. A level of regulation of employee personal information has survived, at least for the 12-month period following the CCPA's effective date (that is, assuming the most recent set of amendment, including AB 25, is signed by the Governor).

In the latest version of AB 25 (with a sigh of guarded relief from employers), employee personal information would be excluded from most of the CCPA's requirements. These include the requirements that permit consumers to request: the deletion of their personal information; the categories of personal information collected; the sources from which personal information is collected; the purpose for collecting or selling personal information; and the categories of third parties with whom the business shares their personal information. This exclusion does not extend to all "employee" data regardless of context. The exclusion applies to personal information collected by a business about a natural person in the course of such person acting as a job applicant to or an employee, owner, director, officer, medical staff member, or contractor of that business, and to the extent the person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to or an employee, owner, director, officer, medical staff member, or contractor of that business.

Importantly, employees of covered businesses still would be entitled to a privacy notice. In addition, employees would be permitted to commence a private right of action if affected by a data breach caused by a failure of the employer to maintain reasonable safeguards.

Under the privacy notice provision, covered businesses would be required to inform employees, as described above, as to the categories of personal information they collect and the purposes for which it will be used. Under the private right of action provision, employees of covered businesses would be permitted to bring an action, including as a class action, if their nonencrypted or nonredacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures. The CCPA's private right of action provision relating to data breaches, which incorporates a narrower definition of personal information, would apply.

This exclusion is temporary and is set to sunset on January 1, 2021, on the understanding that the Legislature would consider more comprehensive employee privacy legislation during the one-year period.

## 6. Does the CCPA apply to businesses only doing business with other businesses, "B2Bs"?

There is no general “B2B” exception under the CCPA. However, many businesses have been concerned about how to handle the personal information of business contacts. That is, the personal information about individuals who are not acting as “consumers” in the general sense but are engaging with a business to carry out certain communications or transactions with the covered business.

Approved at the end of the last legislative sessions, AB 1355 would provide relief from certain CCPA requirements, such as providing notice and granting access and deletion rights for the following personal information:

Personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit or government agency.

This language appears to provide some relief. However, it may not completely close the loop on the personal information of business contacts. For example, initial contacts with such persons, when due diligence has not commenced and there are no products or services to be received at that point, may not be covered by this exception. Additionally, as with the exception for employee information, this relief is temporary — it lasts until January 1, 2021.

## 7. Does the CCPA apply to health information?

The CCPA does not apply to medical information governed by the Confidentiality of Medical Information Act (CMIA) or protected health information collected by a covered entity or business associate governed by the privacy, security, and breach notification rules of the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. While this is welcome news for health care providers, health plans, and their business associates, these exceptions do not exclude these entities from the law, just the type of information described. Thus, a health care provider might still have CCPA obligations, albeit not with respect to protected health information of patients.

## 8. Does the CCPA apply to website cookies?

A cookie is a small text file that a website places on a user’s computer (including smartphones, tablets, and other connected devices) to store information about the user’s activity. Cookies have a variety of uses, ranging from recognizing a user when the user returns to the website to providing advertising targeted to the user’s interests. Depending on their purpose, the website publisher or a third party may set the cookies and collect the information.

The CCPA defines personal information to include a “unique identifier.” This means:

a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology ... or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device.

Therefore, personal information collected by website cookies that identifies or could reasonably be linked to a particular consumer, family, or device may be subject to the same disclosure notices and consumer rights, including the right to delete or opt out of the sale of information to a third party, as other personal information collected through the website.

The CCPA does not require websites of covered businesses to have a separate cookie policy to address the collection and use of personal information through cookies, or to permit consumers to exercise their rights. This information can be included in the website's privacy policy.

Covered businesses may not have a full understanding of what cookies are present on their websites or their functionality. In certain cases, third parties may place cookies on the website that collect personal information as part of services necessary for the site's business purpose. In other cases, it may be unclear if a third- party cookie's collection of personal information is strictly for the website's business purpose or a sale subject to the right to opt out. This may apply in cases where cookies are placed by embedded content (*e.g.,* video), a social media widget, or a vendor that provides targeted or behavioral advertising.

## 9. What obligations do the notice and rights provisions of the CCPA place on businesses?

Question 3 above outlines the notice requirements and rights consumers have under the CCPA, which create obligations for covered businesses. Businesses must provide the notices and be prepared to respond to consumers seeking to exercise their rights.

In the case of providing notice, covered businesses will have to learn more about the data they collect, process, disclose, and sell. For example, they will have to investigate the sources of the personal information they collect and the third parties to whom they share this information. This same information will be needed to assist consumers with carrying out certain of their rights under the CCPA, such as the right to request information about their personal information. Additionally, businesses will have to know where they maintain personal information so that they will be able to carry out a request for deletion, assuming no exception applies.

Before a covered business must actually carry out a consumer's request under the CCPA, it also must make available mechanisms for consumers to submit requests and have a process for verifying the request is valid — a "verifiable consumer requests." It is expected that regulations will provide guidelines for determining verifiable consumer requests. Until then, businesses should apply reasonable procedures for doing so.

In general, covered businesses must make available at least two mechanisms for submitting requests concerning their rights under the CCPA, including, at a minimum, a toll-free telephone number. If the business maintains an internet website, it must make the website available to receive requests. However, a business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information is required to provide only an email address for submitting requests.

The CCPA includes specific timeframes for responding to verifiable consumer requests. When requests for information are made under the CCPA, for instance, businesses generally must respond to verifiable consumer requests within 45 days. That period may be extended as long as the consumer is notified within the first 45-day period. The response must cover the 12-month period preceding the receipt of the request. However, businesses are not required to respond to more than

two requests for the same consumer during a 12-month period. To increase efficiency in responding to requests, the CCPA requires employees designated to handle the responses to these requests be trained.

## 10. Does the CCPA require specific security safeguards to protect consumer personal information?

The CCPA's focus is on the privacy of personal information and extending greater control to individuals over their data. However, security is an element of privacy and while the CCPA does not expressly require implementation of specific security measures, it recognizes a business's duty to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." To do so, organizations typically need to conduct a risk assessment to review the types and sensitivity of its consumer and employee personal information, as well as the risks to the security and privacy of this information. Covered businesses with questions about specific safeguards for maintaining security should refer to the California Attorney General's February 2016 Data Breach Report, which discusses best practices for data safeguarding. Similar frameworks are mandated in other states, such as Colorado, Massachusetts, New York, and Oregon.

The definition of personal information subject to the safeguarding and private right of action provision is much narrower than the general definition of personal information under the CCPA. The CCPA incorporates the definition of personal information applied under the California breach notification law (Cal Civ. Code Section 1798.81.5(d)(1)(A)) set forth below:

(d) For purposes of this section, the following terms have the following meanings:

(1) **"Personal information" means:**

(A) An individual's first name or first initial and his or her 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:

(i) Social security number.

(ii) Driver's license number or California identification card number.

(iii) Account number, 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.

(iv) Medical information.

(v) Health insurance information.

That section goes on to provide that "medical information" means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional. It provides that "health insurance information" means an individual's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

## 11. Can a covered business be sued for violating the CCPA?

The CCPA authorizes a private cause of action against a covered business if a failure to implement reasonable security safeguards results in a data breach. The definition of personal information for this purpose is much narrower than the general definition of personal information under the CCPA.

What should be troubling for covered businesses is that, if successful, a plaintiff can recover statutory damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater, as well as injunctive or declaratory relief and any other relief the court deems proper. This means that plaintiffs in these lawsuits do not have to show actual harm or injury to recover. Thus, in addition to notification obligations a covered business may have under the state's breach notification law, class action lawsuits brought pursuant to this provision of the CCPA could be very costly.

Before a consumer would be able to bring a lawsuit following a covered business's data breach, he or she must provide the covered business 30 days' written notice identifying the specific provisions of the CCPA that were violated. If cure is possible and the covered business actually cures the violation within the 30-day period and provides an express written statement that the violations have been cured and that no further violations will occur, the consumer would not be able to pursue the action for individual statutory damages or class-wide statutory damages. The consumer still could seek actual pecuniary damages suffered as a result of the alleged violations.

## 12. Can service providers be liable?

Under the CCPA, a service provider means a for-profit legal entity that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract. The contract must include several prohibitions. For example, the service provider cannot retain, use, or disclose personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or otherwise specified under the law. Accordingly, covered businesses must carefully review their existing agreements with third-party service providers that are likely to be collecting or processing California consumer information to ensure they include the required language.

A service provider that receives personal information by way of their contractual agreement and uses it in violation of the restrictions under in the CCPA can be liable for those violations. A service provider, however, is not liable for failure by a business that shares personal information with them to comply with its CCPA obligations. For example, a service provider holding personal information provided by a business is not liable for that business's failure to comply with its obligations to delete that personal information upon a consumer's request.

Penalties for a service provider's violations of the CCPA are similar to the those of a business that violates the CCPA. A business or service provider that violates the CCPA can face injunctions and penalties of not more than $2,500 for each violation, and not more than $7,500 for each intentional violation, in an action brought by the California Attorney General. A business or service provider is provided 30 days after receiving written notice of noncompliance to cure the violation, before facing liability.

## 13. Is personal information in M&A considered a "sale" of consumer personal information?

Consumer personal information may be part of business assets transferred to a third party in the course of a merger, acquisition, or bankruptcy when the third party assumes control of all or part of the business. In general, this type of transfer will not constitute a sale of personal information for the purposes of the CCPA. But, if the third party materially alters how it uses or discloses the consumer's personal information and that use or disclosure is materially inconsistent with the notice provided to the consumer at the time of collection, the third party must provide the consumer with prior notice of the changed practices. Parties to the transaction should consider whether to address this issue in the purchase agreement.

## 14. Does the CCPA apply if a consumer is no longer a resident of California?

Depending on the facts, if a consumer moves or is transferred to a location outside of California, the consumer may no longer be a resident of California and his or her personal information will no longer be protected by the CCPA. Businesses must remember, however, that what they say about the handling of personal information may continue to apply even if the law no longer applies. In addition, the consumer's personal information may be protected by the new state of residence or other jurisdiction. Covered businesses should consider this and similar issues when drafting notices for consumers concerning their rights under the CCPA. For example, if a notice extends rights to a "consumer" and not a "consumer who is a California resident," a transfer that would change the person's residency may not change the rights extended in that notice.

## 15. How does the CCPA interact with federal, state, or local laws?

The CCPA provides that its obligations are a matter of statewide concern in California and supersede and preempt all rules, regulations, codes, ordinances, and other laws adopted by a city, county, municipality, or local agency regarding the collection and sale of a consumer's personal information by a business.

However, the CCPA also states that its obligations will not restrict a business's ability to comply with federal, state, local laws, or regulations. In addition, while the CCPA is drafted to supplement federal and state law, it will not apply if it is preempted by or in conflict with federal law, the U.S. Constitution, or the California Constitution. To determine which laws or regulations will govern, an organization must identify all the purposes for which consumer information is collected, processed, and retained. For example, while the CCPA includes a carve out for protected health information collected by HIPAA-covered entities and business associates, this is not as broad as it appears. Covered entities and business associates that are otherwise subject to the CCPA must still evaluate how to handle personal information that is not protected health information.

## 16. What should covered businesses do?

Steps covered businesses should consider taking to comply include:

1. Monitor the status of the CCPA to ensure the business is aware of additional amendments and the regulations that will be issued.

2. Begin staging resources to be able to identify and map the consumer personal information in the business's possession or under the business's control, including for others acting on the business's behalf. Successful compliance activity depends in significant part upon knowledge of what information is collected, who it is collected from, how it is collected, why it is collected,

all purposes for which it is used, all locations where it is stored, and any third party with whom it is shared.

3. Review and identify existing or needed organizational and technical procedures to facilitate compliance with consumer rights under CCPA.

These should include:

- Developing or identifying at least two mechanisms for permitting consumers to exercise their rights to request information on what the business collects, the purposes for which it is used, the third parties with whom it is shared. Mechanisms can include an email address, postal address, website link, toll-free phone number, and so on.

- Developing or identifying internal mechanisms that could be made available to respond to a consumer's exercise of access rights, including verifying identity, responding within the mandated timeframe, and documenting the request and response.

- Developing or identifying an internal mechanism for deleting a consumer's personal information on request. This will include determining whether any state or federal laws preempt the deletion and notifying third parties with whom the business has shared the information to delete the information.

- If applicable, developing or identifying an internal mechanism to track third parties to whom consumer personal information is sold in order to comply with the consumer's request to opt out of that sale.

- Identifying state and federal laws that address record retention and destruction and how they interact with the CCPA and a business's operational needs.

4. Review or create a data retention schedule that reflects the types of data the business maintains. The obligation to safeguard data, both under the CCPA and under Cal. Civ. Code 1798.81.5, is a significant reason to reduce the amount of personal information retained after it is no longer necessary for the purpose for which it was collected.

5. Identify whether the business needs to update notice of collection and processing activities, as well as consumer access and deletion rights. Places where these may reside include the intranet, business website, website privacy policy, employee recruiting platform, and consumer rights notice.

6. Begin identifying the staff who would be responsible for handling consumer access rights and other requests under the CCPA and how the business will train these staff members. It will be important to maintain consistency when carrying out these obligations, as well as documenting the training.

7. Review services agreements with service providers that have access to consumer personal information (such as IT providers, marketing companies, and professional service providers). Contract provisions should address appropriate security safeguards, data breach reporting obligations, use and disclosure limitations, data retention and disposal, and the ability to

assist the business in responding to a consumer rights requests. Covered businesses should be negotiating, reviewing, or renegotiate existing agreements to ensure the service provider's ability to comply with access rights relating to information collected and retained. This practice dovetails with the requirements of Cal. Civ. Code 1798.81.5(c) to contractually require that a third party with whom the business shares personal information maintains reasonable security procedures to safeguard the business's personal information.

8. Review organizational and technical access controls. The CCPA permits a consumer to bring a private cause of action against a business for the unauthorized access and exfiltration, theft, or disclosure of personal information as a result of the business's failure to implement and maintain reasonable security procedures and practices. California's breach notification law excepts from the definition of a breach an unauthorized but good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business, as long as the information is not used or subject to further unauthorized disclosure. However, in permitting a private cause of action for a data breach, it is not clear that the CCPA would apply this exception. Therefore, a covered business may be liable for the unauthorized access of consumer personal information by its employees and agents even if the incident is not a reportable breach under Cal. Civ. Code section 1798.82. To guard against this, businesses should ensure their organizations have appropriate policies and procedures in place, including role-based access, password management, system auditing, and training.

9. Review the business's written information security program (WISP) or internal administrative and technical policies and procedures and ensure they reflect and demonstrate compliance with the CCPA requirements of security safeguards appropriate to the nature of the information to protect the personal information.

## Conclusion

Many of the steps listed above may be adapted to satisfy other data privacy protection frameworks, assist in developing a robust internal data protection program, or position the business for future regulatory obligations. All 50 U.S. states have enacted data breach notification laws. Many have enacted laws addressing data safeguarding, disposal, or vendor management, and many, like Nevada, may begin advancing legislation similar to the CCPA. Several federal data protection laws are under consideration and countries around the world continue enacting national data privacy laws to protect individuals. This legislative activity, combined with the growing public awareness of data privacy rights and concerns, makes the development of a meaningful data protection program an essential component of business operations.



National Law Review, Volumess IX, Number 287