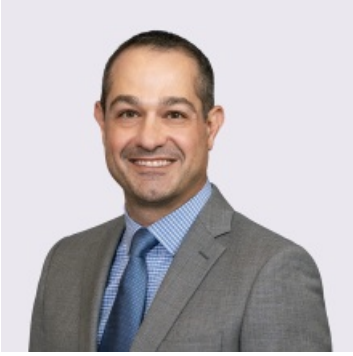
Special Report

California Consumer Privacy Act, California Privacy Rights Act FAQs for Covered Businesses

By Jason C. Gavejian, Joseph J. Lazzarotti, Damon W. Silver, Mary T. Costigan &

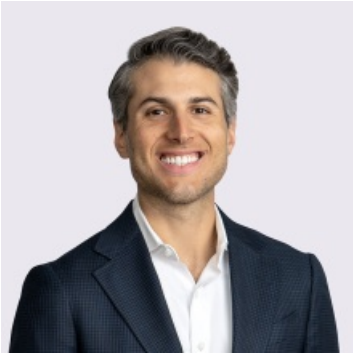
January 19, 2022

Meet the Authors



Jason C. Gavejian
Office Managing Principal
908-795-5139
Jason.Gavejian@jacksonlewis.com

Joseph J. Lazzarotti
Principal
908-795-5205
Joseph.Lazzarotti@jacksonlewis.com



Damon W. Silver
Principal

The California Consumer Privacy Act (CCPA), considered one of the most expansive U.S. privacy laws to date, went into effect on January 1, 2020. The CCPA placed significant limitations on the collection and sale of a consumer's personal information and provides consumers new and expansive rights with respect to their personal information.

Less than one year later, on November 3, 2020, a majority of California residents voted in favor of Proposition 24, which included the California Privacy Rights Act (CPRA). The CPRA builds upon the CCPA's extensive framework of privacy rights and obligations, both expanding and modifying key aspects of the CCPA, and generally becomes effective January 1, 2023.

These FAQs highlight critical CCPA and CPRA compliance requirements. They should help businesses determine whether they are subject to the CCPA/CPRA, and if so, learn more about the obligations they may have and strategies for implementing policies and procedures to comply.

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

1. Which businesses does the CCPA/CPRA apply to?

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

A. Is for profit and does business in the State of California;

B. Collects California resident 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:

- Annual gross revenue in excess of $25 million. The California Attorney General clarified in comments to questions concerning CCPA regulations that this revenue threshold is not limited to revenue generated in California or from California residents. The CPRA further clarified that a business determines whether it satisfies the threshold on January 1 of a year by looking to annual gross revenues in the preceding calendar year.
- 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. The

(212) 545-4063
Damon.Silver@jacksonlewis.com

Mary T. Costigan
Principal
908-795-5135
Mary.Costigan@jacksonlewis.com

Related Services

Biometrics
California Advice and Counsel
California Consumer Privacy Act
Privacy, Data and Cybersecurity

CPRA modified this prong to read "alone or in combination, annually buys, sells, or shares the personal information of *100,000 or more consumers or households*."

- Derives at least 50 percent of its annual revenue from selling consumers' personal information. Under the CPRA, the "sharing" of personal information also counts toward the qualifying threshold.

Businesses located outside of California — the "long arm" of the CCPA/CPRA. A business need not be located in California to be subject to the CCPA/CPRA. While the CCPA/CPRA 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.

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. However, an entity that controls or is controlled by a "business," as defined, may itself qualify if it shares common branding with that business. The CPRA adds that such entity will be treated as a business only if the related business shares consumer personal information with it. Accordingly, entities that would not themselves be a "business" under the CCPA could become subject to the law because the businesses that control them, or that they control, share common branding and consumer personal information with them.

"Control" or "controlled" for this purpose means:

- Ownership of, or the power to vote, more than 50 percent 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.

"Common branding" means a shared name, servicemark, or trademark. Under the CPRA, such common branding must cause the average consumer to understand that the entities are commonly owned.

The CPRA adds a third category that could be a "business" — a joint venture or partnership composed of businesses in which each business has at least a 40 percent interest.

2. What about entities that provide services to businesses covered by the CCPA/CPRA?

The CCPA regulates the "service providers" of a business — *i.e.,* the for profit legal entities that process personal information on behalf of the business and to which the business discloses personal information for a business purpose pursuant to a contract that includes certain terms. The CPRA makes substantial changes to the rules that apply to entities that work with covered businesses to receive and process personal information or that receive personal information from a business.

The CPRA identifies three types of entities:

- Contractors. A “contractor” is a person to whom the business makes available a consumer’s personal information for a business purpose pursuant to a written contract that includes certain provisions. For example, the contract must prohibit the contractor from (i) selling or sharing the personal information and (ii) retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract, or outside the direct business relationship between the contractor and the business.
- Service Providers. A “service provider” is a person that processes personal information on behalf of a business and that receives from or on behalf of the business a consumer’s personal information for a business purpose pursuant to a written contract that includes provisions similar to a contractor. Such written contracts are required to be put in place downstream should a service provider engage any other person to assist in processing personal information for a business purpose on behalf of the business.
- Third Parties. A “third party” is any person other than: (i) the business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer’s current interaction with the business; (ii) a service provider to the business; and (iii) a contractor. As with contractors and service providers, businesses must enter into agreements with the third parties to whom it sells or with whom it shares personal information.

Further discussion of these relationships is beyond the scope of these FAQs. However, businesses will need to better understand these relationships, including the corresponding contract requirements. This includes a contract obligation added by the CPRA for contractors and service providers to implement and maintain reasonable security procedures and practices to protect personal information.

3. 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, or could reasonably be linked, directly or indirectly, with a particular consumer or household. However, 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 or 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.

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 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.

The CPRA expands the definition of personal information to include a category for sensitive personal information. This category includes personal information that reveals:

- A consumer's social security, driver's license, state identification card, or passport number;
- A consumer's account log-In, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
- A consumer's precise geolocation;
- A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;
- The contents of a consumer's mail, email, and text messages, unless the business is the intended recipient of the communication;
- A consumer's genetic data.

Sensitive Personal Information also means:

- The processing of biometric information for the purpose of uniquely identifying a consumer;
- Personal information collected and analyzed concerning a consumer's health; and
- Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

Personal information does not include de-identified or aggregate consumer information. Personal information also does not include publicly available information or, per the CPRA, lawfully obtained, truthful information that is a matter of public concern. Under the CCPA, "publicly available" means information that is lawfully made available from federal, state, or local government records. The CPRA adds to the exclusion information a business has a reasonable basis to believe is lawfully made available (i) to the general public by the consumer or from widely distributed media; (ii) by the consumer; or (iii) information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. It is unclear whether clause (ii) above was intended to remain in the statutory language. The language seems to read that information excluded from the definition of personal information under the CCPA/CPRA includes personal

information made available by the consumer, even if not just to the general public.

4. What rights do consumers have over their personal information under the CCPA/CPRA?

Covered businesses have an obligation to develop programs to manage the sweeping suite of rights the CCPA grants to consumers and which the CPRA expanded. Below is a rundown of those rights:

Notice at Collection. A business that collects (under the CPRA, "controls the collection of") a consumer's personal information must disclose to consumers, at or before the point of collection, (i) the categories of personal information, including sensitive personal information, collected and (ii) the purposes for which the categories are to be used. According to the CPRA, the notice also must include the purposes for which such categories are collected or used and indicate whether that information is sold or "shared" (a newly and broadly defined term under the CPRA, discussed below, the inclusion of which is intended to create greater transparency around, and consumer control over, businesses' use of personal information for cross-context behavioral advertising). The CPRA also requires the notice to include information about how long each category of personal information, including sensitive personal information, will be retained.

In either case, after the notice has been provided, the business may not collect additional categories of personal information or use personal information collected (or sensitive personal information under the CPRA) for additional purposes that are incompatible with the purposes disclosed in the notice without providing the consumer renewed notice.

Privacy Policy. 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 how they may exercise those rights. These disclosures must be updated, as applicable, every 12 months. Under the CPRA, these privacy policies will have to be updated to include the new and modified consumer rights highlighted below.

Right to Know. The CCPA grants consumers the right to request information regarding:

- The categories of personal information businesses collect about them (*see, e.g.,* the categories above);
- The categories of sources from which that personal information was collected (*e.g.,* the consumer directly, advertising networks, internet services providers, data analytics providers, government entities, data brokers, and so on);
- The business or commercial purposes for which personal information was collected or sold (*e.g.,* fraud prevention, marketing, or improving customer experience);
- The categories of third parties to whom personal information was disclosed (*e.g.,* advertising networks, internet service providers, government entities, social networks, and so on); and
- The "specific pieces" of personal information collected.

Consumers have the right to request additional information from businesses that sell or share their personal information or disclose it for a business purpose. Specifically:

- The categories of personal information that the business sold about the consumer

and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each category of third parties.
- The categories of personal information that the business disclosed about the consumer for a business purpose and, per the CPRA, the categories of persons to whom it was disclosed for a business purpose.

Where this right to know relates to the sale or selling of personal information, the CPRA generally extends it to sharing. The CPRA defines sharing personal information generally to mean sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating, regardless of the means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration. The CPRA also calls for regulations that may expand access rights with respect to automated decision-making technology and processes, including description of the likely outcomes of the processes with respect to the consumer.

When responding to a verified request for specific pieces of personal information, the CPRA requires the business to provide the specific pieces in a format easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format that can be transmitted to another entity at the consumer's request without hindrance. The CPRA also clarifies that "specific pieces of information" do not include data generated to help ensure security and integrity or as may be prescribed by regulation. Additionally, transferring personal information from one business to another in the context of switching services at the consumer's direction is not considered a disclosure under the CPRA.

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." The CPRA opens the door to a longer lookback period if certain regulatory action is taken. In that case, upon a consumer's request, a business would be required to disclose the requested information beyond the 12-month period, unless doing so would be "impossible or involve a disproportionate effort." However, in this case, the requirement to provide information beyond the 12-month period would apply only to information collected on or after January 1, 2022.

Deletion. With some exceptions, the CCPA permits consumers to request that covered businesses, and their service providers, contractors, and third parties, as applicable, delete personal information collected about them. Contractors and service providers are required to cooperate with the business in responding to the requests and, at the request of the business, are required to delete or enable the business to delete the information required under the law.

Examples of exceptions from the deletion requirement include situations when it is reasonably necessary to maintain the personal information to (i) complete the transaction for which it was collected and (ii) comply with a legal obligation, such as a record retention requirement. The CPRA modifies some of these exceptions. It also clarifies that service providers and contractors need not comply with deletion requests submitted by the consumer to them directly when the service provider or contractor

collected, used, processed, or retained the personal information in its role as a service provider or contractor to the business.

Correct Inaccurate Information. The CPRA expands consumers' rights with respect to their personal information to include the right to request that a business correct the consumer's personal information if it is inaccurate. Covered businesses must disclose this new right to consumers and use "commercially reasonable efforts" to correct personal information upon receiving a verifiable consumer request.

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. The CPRA adds a similar right for consumers to opt out of the sharing of their personal information. The CPRA also provides for regulatory activity that would empower consumers to opt out of the use of automated decision-making technology in connection with decisions about the consumer's work performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

Limit Use. For businesses that collect "sensitive personal information" (see above), the CPRA grants consumers the right to direct those businesses to limit the use and disclosure of certain sensitive personal information to uses necessary to provide the products and services reasonably expected by the consumer requesting them, and for certain other purposes. This right is limited to sensitive personal information collected or processed for the purpose of inferring characteristics about the consumer. Businesses also should expect regulations that have the goal of strengthening consumer privacy, but that will also consider legitimate operational interests of businesses. To facilitate consumers' exercise of this right, covered businesses must provide a "Limit the Use of My Sensitive Personal Information" link on their internet homepages, which enables consumers to exercise this right.

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 their 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.

The CPRA expands nondiscrimination protections in the employment context by prohibiting businesses from retaliating against an employee, applicant for employment, or independent contractor for exercising their rights under the CCPA/CPRA.

5. Can consumers waive their rights?

No. The CCPA (including as amended by the CPRA) 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.

6. Does the CCPA apply to employee/applicant data?

Employee personal information has been a highly contested matter throughout the CCPA's amendment process. A level of regulation of employee/applicant personal information has survived and will be extended at least until the CPRA effective date, January 1, 2023.

As of now, employees of and applicants for employment with covered businesses have limited rights. They are (1) entitled to a notice at collection, as described above, and (2) empowered to file lawsuits — including class actions — if their personal information, which is more narrowly defined in this context, is affected by a data breach caused by an alleged failure of their employer to maintain reasonable safeguards.

Aside from the above, the CCPA excludes employee and applicant personal information 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 employment-related data, however, regardless of context. Instead, it applies only 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 (collectively, for simplicity, "employees"), 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.

The employee/applicant exclusion is temporary and is set to sunset on January 1, 2023, when the CPRA becomes effective. If the CPRA is not amended to extend the exemption beyond December 31, 2022, employees, applicants, independent contractors, and certain others will receive all the same rights consumers have under the CCPA. If so, on and after January 1, 2023, businesses subject to the CCPA, for example, will not be able to discriminate against their California employees if they decide to exercise their right to know, right to delete, right to opt-out, as well as new CPRA rights — *e.g.,* to restrict disclosure and limit use of, and request corrections to, personal information.

7. 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 who are not traditional consumers. 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.

A bill adopted in 2019, AB 1355, provides some relief by excluding from the CCPA 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 acted or is acting as an employee, owner, director, officer, or independent 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. (updated for CPRA)

This language appears to address some concerns of businesses that primarily do business with other businesses, and not individual consumers. 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 not yet products or services to be received, may not be covered by this exception. Additionally, as with the exception for employee information, this relief is temporary — it lasts until January 1, 2023, when the CPRA becomes effective.

8. 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 healthcare providers, health plans, and their business associates, these exceptions do not exclude them from the law entirely; instead, it provides relief only to the extent the information at issue is subject to those laws (*e.g.,* to protected health information under HIPAA). Thus, a healthcare provider might still have CCPA obligations, albeit not with respect to protected health information of patients.

Additionally, these exclusions need to be reviewed carefully as they may not cover all medical information a business might collect. For example, when applying safety measures for COVID-19, medical information collected from employees and others may not fall under the definition of "medical information" under the CMIA or "protected health information" under HIPAA.

While the CPRA makes minor changes to the exclusion for information collected as part of clinical trials, it leaves the exclusion for medical information unchanged.

9. Does the CCPA apply to website cookies?

A cookie is a small text file 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.

This definition is largely unchanged by the CPRA. 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.

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

Question 3 above outlines the basic notice and policy requirements for businesses and the rights consumers have under the CCPA, as amended by the CPRA. Meeting those requirements and being prepared to respond to consumers seeking to exercise their rights inherently requires measures beyond notices and policies. Of course, some updating those notices and policies will be necessary for the CPRA. For example, many businesses will need to augment their notices at collection to:

- Disclose whether they sell or share personal information;
- Address the collection, processing, and disclosure of "sensitive personal information," a new category of information created by the CPRA (see above);
- Specify how consumer may exercise their right to correct inaccurate personal information; and
- Explain record retention time frames for each category of personal information.

Necessary to preparing notices and privacy policies, covered businesses need to fully understand the data they collect, process, disclose, share, and sell. To outline the categories of sources of personal information they collect and the third parties to whom they share this information, for instance, they must understand what personal information they have, how they obtained it, and under what circumstances they disclose, share, or sell it. Similar information will be needed to respond to consumers as they carry out their rights under the CCPA/CPRA, such as the right to know and the right to limit the use of their sensitive personal information. Additionally, businesses will have to know where they maintain personal information so they will be able to carry out

a request for deletion, assuming no exception applies. This includes, for example, knowing which contractors, services providers, and third parties may process or possess their personal information.

Before a covered business must actually carry out a consumer's request under the CCPA/CPRA, it also must make available mechanisms for consumers to submit requests and have a process for verifying the request is valid — a "verifiable consumer request." 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/CPRA, for instance, businesses generally must respond to verifiable consumer requests within 45 days (businesses must confirm receipt of the request within 10 business days of receipt). That period may be extended as long as the consumer is notified within the first 45-day period. However, businesses are not required to respond to more than two requests regarding the right to know 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.

11. Does the CCPA/CPRA 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 did not expressly require implementation of specific security measures, the CPRA does. The CPRA adds subsection (e) to section 1798.100:

> A business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Section 1798.81.5.

California Civil Code section 1798.81.5 requires a business that:

> owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

The CPRA also calls for additional regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to (i) perform a cybersecurity audit on an annual basis, and (ii) submit to the California Privacy Protection Agency on a regular basis a risk assessment concerning the processing of personal information. This risk assessment must:

- Include whether the processing involves consumers' sensitive personal information

(see Question 3 above); and
- Identify and weigh the benefits to the business, consumer, other stakeholders, and the public from the processing against the potential risks to the rights of the consumer whose data is being processed.

These regulations must be adopted by July 1, 2022, and likely will provide further guidance on the scope of, and process for, conducting and documenting risk assessments. Covered businesses with questions about specific safeguards for maintaining security may consider referring 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 for data breaches is narrower than the general definition of personal information under the CCPA/CPRA. The CCPA incorporates the definition of personal information applied under Cal. Civ. Code Section 1798.81.5(d)(1)(A):

> (1) "Personal information" means either of the following:
>
> > (A) 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:
> >
> > > (i) Social security number.
> > >
> > > (ii) 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.
> > >
> > > (iii) 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.
> > >
> > > (iv) Medical information.
> > >
> > > (v) Health insurance information.
> > >
> > > (vi) 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.
> > >
> > > (vii) Genetic data.

The CPRA adds to this clause (B) of that definition: a username or email address in combination with a password or security question and answer that would permit access to an online account. Although narrower than the general personal information definition, these obligations apply to a broad set of data. For example, "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 healthcare professional.

12. Can a covered business be sued for violating the CCPA/CPRA?

The CCPA authorizes a private cause of action against a covered business if its failure to implement reasonable security safeguards (as provided in Question 11 above) results in a data breach affecting personal information.

Significantly, 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 may 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/CPRA could be very costly.

Before a consumer would be able to bring a lawsuit following a covered business's data breach, they must provide the covered business 30 days' written notice identifying the specific provisions of the CCPA/CPRA 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 is not required to provide 30-day notice if the consumer is solely seeking actual pecuniary damages suffered as a result of the alleged violations. Importantly, the CPRA clarifies:

> The implementation and maintenance of reasonable security procedures and practices pursuant to Section 1798.81.5 *following* a breach does not constitute a cure with respect to that breach.

(Emphasis added.)

Accordingly, efforts to mitigate CCPA litigation risk must be proactive —*i.e.,* businesses must leverage their pre-breach maintenance of reasonable safeguards as a defense to the alleged lawsuit, rather than attempting to rely on post-breach remedial action as a cure.

13. Can contractors and service providers be liable?

Question 2 above summarizes some key issues for contractors and service providers under the CCPA/CPRA. In particular, the CPRA includes several new obligations and clarifications for service providers and contractors.

Service providers and contractors must cooperate with the business with regard to responding to verifiable consumer requests. For example, at the direction of the business responding to verified consumer requests, service providers and contractors must delete, or enable the business to delete, personal information. In turn, they also need to notify their own service providers or contractors to delete information subject to such requests. Contractors and service providers also must agree to notify businesses if they cease to be able to meet applicable CPRA obligations. They also must notify businesses if they engage subprocessors to process personal information. These

are just some of the obligations in the CCPA/CPRA applicable to service providers and contractors.

Service providers and contractors that receive personal information by way of their contractual agreement and use it in violation of the restrictions under the CCPA/CPRA can be liable for those violations. However, service providers and contractors are not liable for failure by a business that shares personal information with them to comply with the business's CCPA/CPRA 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 or contractor's violations of the CCPA/CPRA are similar to the those of a business that violates the CCPA/CPRA. A service provider or contractor 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. Service providers and contractors may have an opportunity to cure the violation before facing liability.

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

Consumer personal information may be a business asset 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. The CPRA extends similar treatment to the sharing of personal information in this context.

15. Does the CPRA create a record retention requirement?

The CPRA does not establish specific record retention periods for personal information. However, under the CPRA, a business cannot retain a consumer's personal information for longer than is reasonably necessary for the stated purpose it was collected. A failure to implement and comply with an appropriate data retention and disposal schedule may result in a violation of the CPRA's storage limitation principle. Further, as noted above, businesses must include in their notices at collection the "length of time the business intends to retain each category of personal information, including sensitive personal information" that it collects. If it is not possible for a business to provide consumers with a specific retention period, the business is required to provide consumers with the "the criteria used to determine such period ...." In addition, courts and enforcement bodies may view storage limitation practices as a basic reasonable safeguard and the failure to implement or follow such practices may therefore expose businesses to regulatory and litigation risk.

16. 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 their 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 another 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 move or transfer that would change the person's residency may not change the rights extended in that notice.

17. 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/CPRA 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.

18. What should covered businesses do?

Covered businesses that became compliant with the CCPA by its effective date, January 1, 2020, are likely in the best position to update and expand their CCPA programs to incorporate the CPRA changes. Other businesses will need to move quickly to address the remaining CCPA issues and address the CPRA changes. Of course, there are several considerations, not the least of which is marshaling the resources to address compliance while many businesses are still facing considerable compliance and related issues stemming from the COVID-19 pandemic.

However positioned a business is to achieve compliance, they need to be on the lookout for a bunch of new regulations. The CPRA establishes the new California Privacy Protection Agency (CPPA) and one of its chief responsibilities is drafting CPRA regulations, which could include updating existing CCPA regulations. Under the CPRA, the timeline for adopting final regulations is July 1, 2022. It is unclear, however, when final regulations will be in place. The CCPA regulations' notice and comment process took some time.

Below is a series of steps covered businesses should consider taking as they work toward compliance:

1. Monitor CCPA/CPRA legislative activity to ensure the business is aware of additional amendments, as well as regulations expected to be issued in the first half of 2022.

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. Businesses that completed this step gearing up for CCPA may need to update its mapping for changes in business processes and the like. Successful compliance activity depends in significant part upon knowledge of what information is collected (including, for compliance with the CPRA, what sensitive 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, how long it is maintained, and any third party with whom it is shared.

3. Review and identify existing or needed organizational and technical procedures to facilitate compliance with responding to requests from consumers concerning their CCPA/CPRA rights.

These should include:

- Confirming at least two mechanisms for permitting consumers to exercise their rights to request information.
- Reviewing and evaluating internal mechanisms for verifying identity, responding within the mandated timeframes, and documenting the request and response.
- Assessing contractor, service provider, and third-party preparedness for responding to consumer rights requests, such as right to delete, and pushing those requests downstream.
- If applicable, developing or identifying internal mechanisms to track third parties to whom consumer personal information is sold or shared in order to comply with the consumer's request to opt out of that sale or sharing.
- Identifying state and federal laws that address record retention and destruction and how they interact with the CCPA and a business's operational needs.
- Evaluating the application of similar laws, such as the Colorado Privacy Act (CPA) and the Virginia Consumer Data Protection Act (VCDPA).

4. Update the business' notices, policies, forms, etc. The CPRA will require significant changes to the business' notices at collection, website privacy policy, communications to consumers concerning their rights, and other materials and communications. This may include updated notices to employees, applicants, and others.

5. Identify contractors, service providers, and third parties and evaluate whether compliant contract provisions are in place. Covered businesses should be negotiating, reviewing, or renegotiate existing agreements as soon as possible to ensure agreements are timely in place.

6. Update the training required for staff responsible for handling consumer rights requests to reflect the CPRA changes. It will be important to maintain consistency when carrying out these obligations, as well as documenting the training.

7. Review or create a data retention schedule that reflects the types of data the business maintains. The obligation to safeguard data under the CCPA/CPRA and beyond 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.

8. Review the adequacy of the business's safeguards to protect personal information. This step is imperative if only to help prevent cyberattacks such as ransomware and

email compromise. Adding to that motivation, the CPRA expressly establishes the obligation to so do and may also require regular submissions of risk assessments to the CPPA. As noted, the failure to do so could support a consumer's private cause of action if such failure led to the unauthorized access and exfiltration, theft, or disclosure of 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 have advanced legislation similar to the CCPA. See the CPA and the VCDPA mentioned above. Several federal data protection laws are also 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.

Please contact a Jackson Lewis attorney or the CCPA Team with any questions.