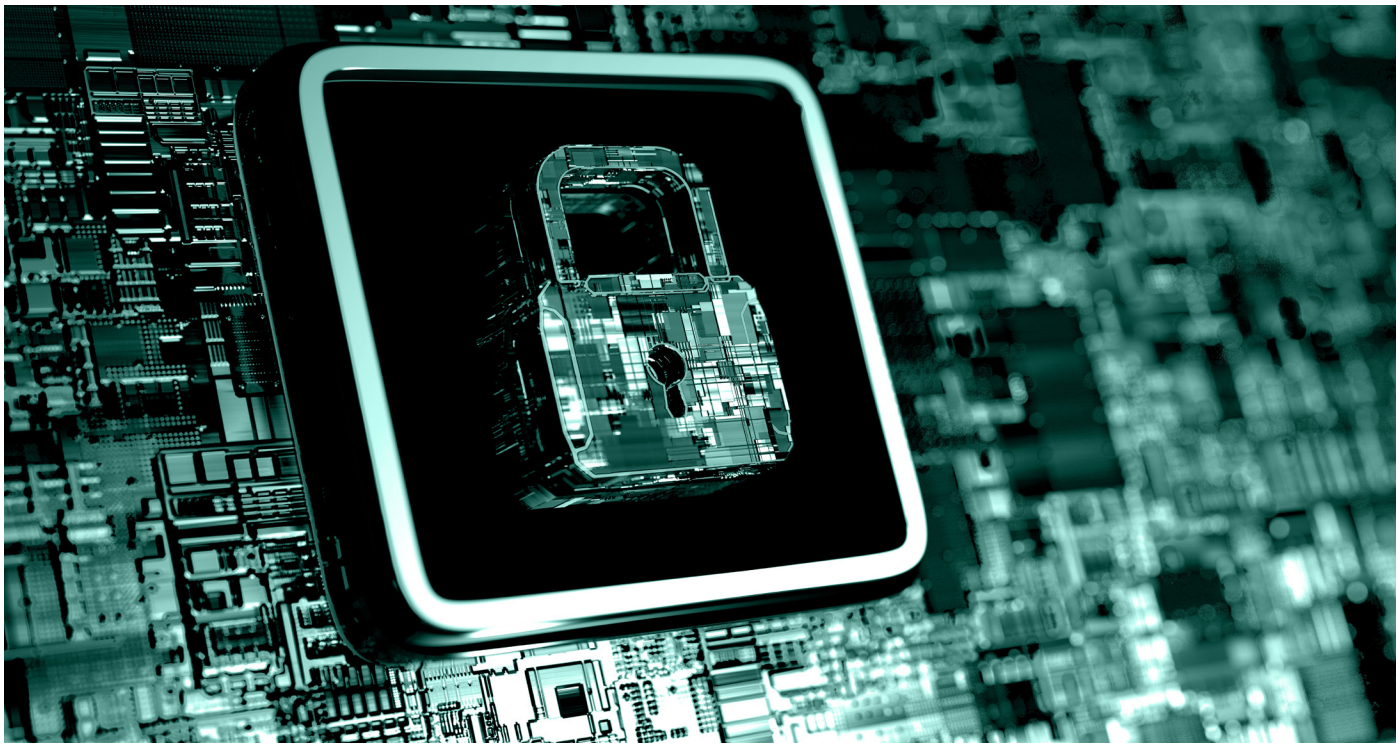
SHIPMAN



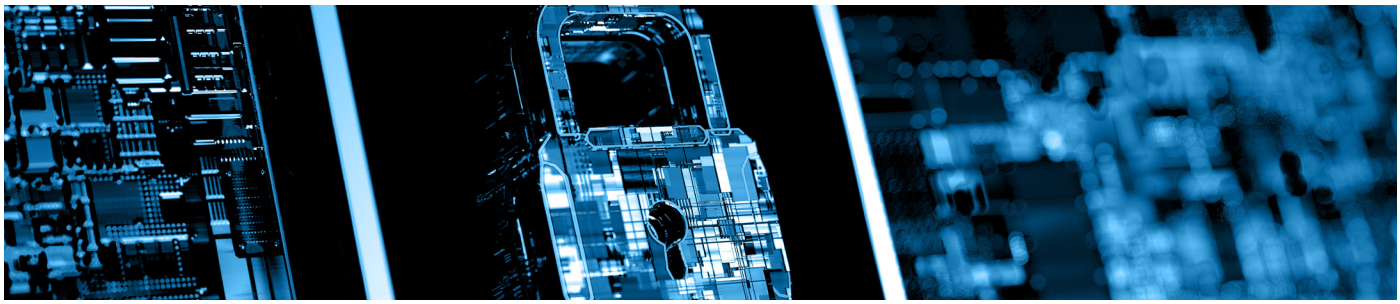
California Privacy Rights Act: A Compliance Guide

June 2021

Prepared by

Shipman & Goodwin LLP

Table of Contents



Overview

On November 3, 2020, California voters passed Proposition 24, the California Privacy Rights Act (CPRA), by a margin of approximately 56% to 44%. By this vote, California has decided to amend and supersede the groundbreaking and still new California Consumer Privacy Act (CCPA), which came into effect on January 1, 2020. The CPRA will supersede the CCPA effective January 1, 2023. Until that time, the CCPA remains in effect.

Background

Many readers may be scratching their heads regarding why California would replace the CCPA so quickly, and, thus, some background on how we arrived at the CPRA would be useful. In 2018, Californians for Consumer Privacy sponsored a ballot initiative to place a new privacy law on the November 2018 California ballot. After obtaining the requisite signatures to qualify for the ballot, Californians for Consumer Privacy negotiated a legislative deal whereby it withdrew the initiative in exchange for the legislature passing the CCPA. The CCPA though was less restrictive than the law originally proposed by the ballot initiative; and, thus, Californians for Consumer Privacy began a process to modify the CCPA and expand potential enforcement.

The result of this process is an extensive and detailed piece of legislation. In its more than 50 pages, the CPRA makes revisions both significant and minor to the CCPA, including alteration to the law's application, creating a new oversight agency (CalPPA), expanding breach reporting obligations, and enhancing individual private causes of actions.

> "...One of the nation's most expansive and strict data privacy laws."

The Compliance Guide

We prepared this Compliance Guide for two purposes - provide brief summaries of the CPRA's key provisions and encourage businesses (in California or otherwise) to begin planning for what will be one of the nation's most expansive and strict data privacy laws. In the first section of this guide, "Key Topics," we address the law's application, review key concepts, and summarize some of the law's more noteworthy and important provisions. In subsequent sections, we provide a general timeline of key dates and deadlines relating to the CPRA's implementation. We end with a compliance checklist for businesses regarding how to approach planning for and complying with the CPRA.

Compliance Guidelines: Key Topics

SHIPMAN

Who Needs to Comply with the CPRA?

The CPRA applies to any entity organized and operated for profit or financial benefit that:

- collects consumers' personal information,
- determines the purpose and means of processing that information,
- does business in the state of California, and
- meets one or more of the following thresholds: 1) has annual gross revenue in excess of 25 million, adjusted for inflation, 2) annually buys, sells, or shares the personal information of 100,000 or more consumers or households, or 3) derives 50% or more of its annual revenues from selling, or sharing consumers' personal information.

Those readers familiar with the CCPA will note that the above criteria differ in that the second threshold in the last bullet point was changed from 50,000 or more consumers, households or devices to 100,000 consumers or households. While the increase from 50,000 to 100,000 may not materially affect the CPRA's application to many businesses, the removal of "devices" is a potentially significant change.

My business is not located in California - do I really need to comply?

While the CPRA's definition of "does business" is broad, CPRA compliance is not required if every aspect of a business's commercial conduct takes place wholly outside of California. Commercial conduct takes place wholly outside of California if:

- The business collected that information while the consumer was outside of California,
- No part of the sale of the consumer's personal information occurred in California, and
- No personal information collected while the consumer was in California is sold.

Therefore, if a California resident provides information to a business outside of California, and that business neither conducts commercial activity in California nor sells that information in California, the CPRA is inapplicable.

Who Is a California Resident?

The CPRA applies to the personal information of California residents, which the law refers to as "consumers."

A consumer is a natural person who is a California resident, as it is defined in the California tax regulation. According to California tax provisions[1], a resident is defined as:

- An individual who is in California for other than a temporary or transitory purpose; and
- An individual domiciled in the state of California who is outside of the state for a temporary or transitory purpose.

As shown above, the definition of a California resident is quite broad. When analyzing whether a purpose is "temporary or transitory," businesses should take into account a number of factors unique to each case.

1 Section 17014 of Title 18 of the California Code of Regulations.

What Is Personal Information?

The CPRA has a very broad definition of "personal information." For a business to decide whether it needs to comply with this law, it has to identify the type of information collected and whether it is, in fact, "personal information."

The CPRA defines personal information as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number or other similar identifiers.
- Personal information including signature, physical characteristics or description, telephone number, state identification card number, insurance policy number, employment, employment history, bank account number, credit card number, debit card number or any other financial information, medical information or health insurance information.
- Characteristics of protected classifications under California or federal law.
- Commercial information, such as records of personal property, products or services purchased.
- Biometric information, meaning an individual's physiological, biological or behavioral characteristics, including DNA, used or intended to be used, separately or in combination with other data, to establish individual identity.
- Internet or other electronic network activity information.
- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Education Rights and Privacy Act.[2]
- Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

2 20 U.S.C. Section 1232g, 34 C.F.R. Part 99.

What is Sensitive Personal Information?

The CPRA also includes a new sub-category of personal information referred to as "sensitive personal information." This sub-category includes government-issued identifiers, such as SSN, Driver's License, etc.; account credentials; financial information; precise geolocation; race or ethnic origin; religious beliefs; contents of certain types of messages; genetic data; biometric information; and other types of information.

Exceptions to the Personal Information Definition

The CPRA excludes the following from the definition of personal information:

- "Deidentified Information" which means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, provided that the business that possesses the information:
  - Takes reasonable measures to ensure that the information cannot be associated with a consumer or household;
  - Publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision; and
  - Contractually obligates any recipients of the information to comply with all provisions of this subdivision.
- "Aggregate Consumer Information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. It does not mean one or more individual consumer records that have been deidentified.

What Does It Mean to "Collect," "Sell," or "Share" Personal Information?

A few key definitions from the CPRA that are used in this Compliance Guide are:

- **"Collect"** means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.

- **"Profiling"** means any form of automated processing of personal information to evaluate personal aspects of an individual and to make predictions concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

- **"Sell"** means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration.

- **"Share"** means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other 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, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

The CPRA enumerates certain exceptions for the definition of sell and share, listed as follows:

- A consumer uses or directs the business to intentionally disclose personal information; or intentionally interact with one or more third parties;

- The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purpose of alerting that the consumer has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information; or

- The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with the CPRA. If the acquirer materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with promises made when collecting the information, it must provide notice of the new or changed practice to the consumer.

Summary of Information to Be Included in Privacy Policies

Under the CPRA, certain information must be included in a business's online privacy policy and in any California-specific description of consumers' privacy rights. If a business does not maintain such policies, this information must be included somewhere on its website. Note that this information must be updated at least once every twelve (12) months.

The following information is required to be included:

- a description of a consumer's rights to:
  - know, at or before the point of collection, the categories of personal information collected by a business, the purposes for which such information is collected or used, and whether such information is sold or shared, as well as information regarding the length of time a business intends to retain each category of personal information;
  - request deletion of any personal information about the consumer that the business has collected from the consumer;
  - request correction of inaccurate personal information;
  - request disclosure of information collected, including specific pieces of personal information a business has collected about the consumer;
  - request disclosure of information sold or shared;
  - opt-out of the sale or sharing of the consumer's personal information (and a link to or statement regarding such option, as applicable); and
  - nondiscrimination relating to the consumer's exercise of his or her rights under the CPRA.
- two or more designated methods for submitting requests permitted under the CPRA, including, at a minimum, a toll-free telephone number.

  Note: A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests permitted under the CPRA. In addition, a business that maintains a website must make the website available to consumers to submit requests permitted under the CPRA.
- a list of the categories of personal information a business has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in the CPRA that most closely describe the personal information collected;
- a list of the categories of sources from which consumers' personal information is collected;

- the business or commercial purpose for collecting or selling or sharing consumers' personal information;
- the categories of third parties to whom the business discloses consumers' personal information; and
- two separate lists:
  - a list of the categories of personal information the business has sold or shared about consumers in the preceding 12 months by reference to the enumerated category or categories in the CPRA that most closely describe the personal information sold or shared (note: if the business has not sold or shared consumers' personal information in the preceding 12 months, the business must prominently disclose that fact in its privacy policy); and
  - a list of the categories of personal information the business has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in the CPRA that most closely describes the personal information disclosed (note: if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business must disclose that fact).

The "Business Purpose" Exception

Throughout the CPRA, there are references to a "business purpose." Notably, a "business purpose" use is not exempt from compliance with the CPRA requirements. For example, consumers have the right to disclosure of the categories of personal information that the business disclosed about the consumer for a business purpose and the categories of persons to whom the information was disclosed for a business purpose. In addition, a business that collects a consumer's personal information and that discloses it to a Service Provider or Contractor for a business purpose must enter into an agreement with such third party, Service Provider, or Contractor, that contains certain provisions prescribed under the CPRA. However, certain provisions of the CPRA do not apply when personal information is disclosed for a business purpose, including the consumer's right to opt-out of the disclosure of personal information.

> **"A 'business purpose' means the use of personal information for the business's operational purposes, or other notified purposes, or for the Service Provider or Contractor's operational purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed or for another purpose that is compatible with the context in which the personal information was collected."**

The CPRA provides the following list of activities that constitute a "business purpose":

- auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards;
- helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes;
- debugging to identify and repair errors that impair existing intended functionality;
- short-term, transient use, including but not limited to non-personalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business;
- performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business;
- providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer, provided that for the purpose of advertising and marketing, a Service Provider or Contractor shall not combine the personal information of opted-out consumers which the Service Provider or Contractor receives from or on behalf of the business with personal information which the Service Provider or Contractor receives from or on behalf of another person or persons, or collects from its own interaction with consumers;

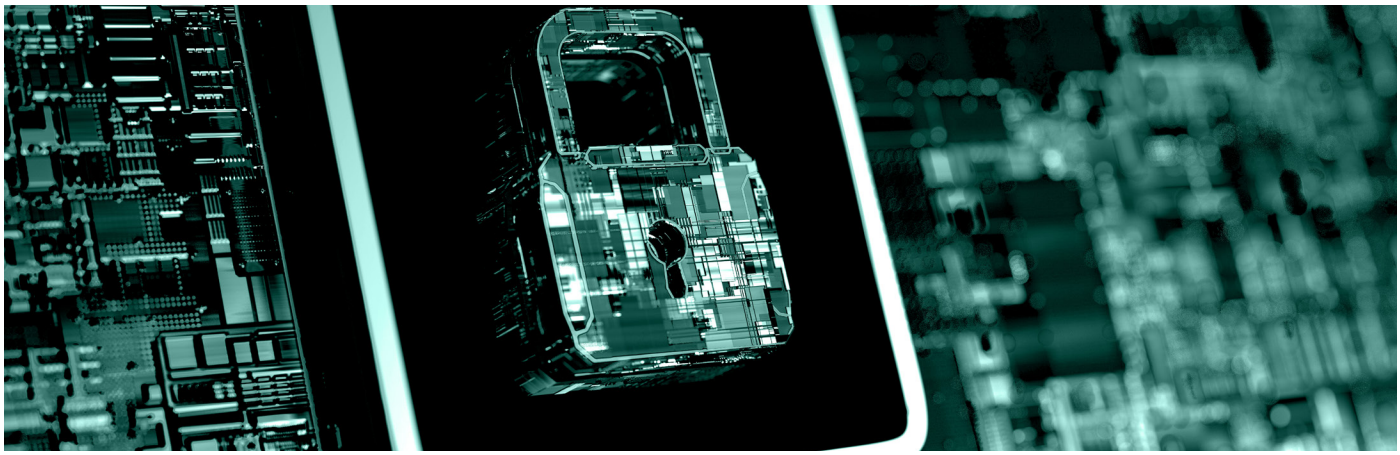
- undertaking internal research for technological development and demonstration; and

- undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

The Research Exception

A business is not required to comply with a consumer's request to delete the consumer's personal information if compliance with such request is likely to render impossible or seriously impair the ability of the business to engage in public or peer-reviewed scientific, historical, or statistical research. This exception applies if the business: (i) obtained the consumer's informed consent for this purpose and (ii) the research otherwise complies with all other applicable ethics and privacy laws. In addition, research with personal information must be:

- compatible with the business purpose for which the personal information was collected;
- subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, by a business;
- made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain, other than as needed to support the research;
- subject to business processes that specifically prohibit reidentification of the information, other than as needed to support the research;
- made subject to business processes to prevent inadvertent release of deidentified information;
- protected from any reidentification attempts;
- used solely for research purposes that are compatible with the context in which the personal information was collected; and
- subjected by the business conducting the research to additional security controls that limit access to the research data to only those individuals as are necessary to carry out the research purpose.



Exemptions

There are several exemptions listed in the CPRA and we have highlighted some of these exemptions below. Among other things, the CPRA does ***not*** apply to:

Medical Information... medical information governed by the Confidentiality of Medical information Act (the "CMIA") or protected health information ("PHI") that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules established pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH");

Provider of health care or a covered entity... a provider of health care governed by the CMIA or a covered entity governed by HIPAA, to the extent the provider or covered entity maintains patient information in the same manner as medical information or PHI under the CMIA, HIPAA, and HITECH;

Personal Information... personal information collected as part of a clinical trial or other biomedical research study subject to or conducted in accordance with the Federal Policy for the Protection of Human Subjects (also known as the Common Rule) pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration ("FDA"), provided that such information is not sold or shared in a manner not permitted by the aforementioned rules and guidelines, and if it is inconsistent, that participants be informed of such use and provide consent;

Vehicle Information... vehicle information or ownership information retained or shared between a new motor vehicle dealer, as defined in Section 426 of the Vehicle Code, and the vehicle's manufacturer, as defined in Section 672 of the Vehicle Code, if the vehicle or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall conducted, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose;

Credit Information

activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or by a furnisher of information, who provides information for use in a consumer report, and by a user of a consumer report (note: this exemption applies only to the extent that such activity involving the collection, maintenance, disclosure, sale, communication or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act ("FCRA") and the information is not collected, maintained, used, communicated, disclosed, or sold except as authorized by the FCRA);

Personal Information...

personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act ("GLBA") and implementing regulations, the California Financial Information Privacy Act ("FIPA"), or the Federal Farm Credit Act of 1971 and implementing regulations;

personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 ("DPPA");

personal information that is collected by a business about a person in the course of the person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of that business to the extent that the person's personal information is collected and used by the business solely within the context of the person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or an independent contractor of that business;

personal information that is collected by a business that is emergency contact information of a person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of that business to the extent that the personal information is collected and used solely within the context of having an emergency contact on file;

personal information that is necessary for the business to retain to administer benefits for another person relating to the person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of that business to the extent that the personal information is collected and used solely within the context of administering those benefits;

Personal Information... personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a person who acted or is acting as an employee, owner, director, officer, or independent contractor of a company, partnership, sole proprietorship, non-profit, 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, non-profit, or government agency. (note that this exemption applies only to the obligations imposed on businesses relating to providing information regarding the categories of information collected, used, sold, or shared; requests for deletion of personal information; requests for correction of inaccurate personal information; requests for access to personal information; requests to know what personal information is shared or sold; requests to limit use and disclosure of sensitive personal information; and limiting the sale, sharing, and use of personal information).

Note: the carve-outs for information collection under the FCRA, GLB, FIPA, the Federal Farm Credit Act of 1971, and DPPA do not apply to the right to bring a private action for a data security breach.

Note: the carve-outs for information collected about job applicants to, employees of, owners of, directors of, officers of, medical staff members of, or independent contractors of a business become inoperative on January 1, 2023.

Individual Rights: *Access*

A consumer has the right to request that a business disclose to the consumer the following:

1. the categories of personal information it has collected about that consumer;
2. the categories of sources from which the personal information is collected;
3. the business or commercial purpose for collecting, selling, or sharing personal information;
4. the categories of Third Parties to whom the business discloses personal information; and
5. the specific pieces of personal information it has collected about that consumer.

Verifiable Consumer Requests

A business must only provide this information upon receipt of a "Verifiable Consumer Request" ("VCR"), which is a request that permits the business to reasonably verify that the individual making the request is the consumer, or an individual authorized to act on behalf of the consumer, about whom the business has collected personal information.

A business must make available to consumers two (2) or more designated methods for submitting requests, including, at a minimum, a toll-free telephone number; and if a business maintains an internet website, it must make the internet website available to consumers to submit requests. However, a business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information is only required to provide an email address for submitting requests.

Responding to a Verifiable Consumer Request

Timeframe for Response

A business that receives a VCR must disclose any personal information it has collected about a consumer, directly or indirectly, including through or by a Service Provider or Contractor, to the consumer. A business is required to disclose and deliver the required information to a consumer, free of charge, within forty-five (45) days of receiving a VCR from the consumer. This time period may be extended once by an additional forty-five (45) days when reasonably necessary, so long as the consumer is provided notice of the extension within the first 45-day period.

Delivery Method

A business's disclosure of the required information must be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, "in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance." Although a business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, it must not require the consumer to create an account with the business in order to make a VCR. However, in the event the consumer has an existing account with the business, the business may require the consumer to use that account to submit a VCR.

Applicable Time Period

The information provided must cover the 12-month period preceding the business's receipt of the VCR. A consumer may request that the business disclose the required information beyond the 12-month period (limited to personal information collected on or after January 1, 2022), and the business is required to provide that information unless doing so proves impossible or would involve a disproportionate effort. There is no obligation to provide this information to the same consumer more than twice in a 12-month period.

Individual Rights: *Knowledge of Personal Information Collected, Shared, and Sold*

A consumer has the right to request that a business that sells or shares the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

1. the categories of personal information that the business collected about the consumer;
2. the categories of personal information that the business sold or shared about the consumer and the categories of Third Parties to whom the personal information was sold or shared, by category or categories of personal information for each category of Third Parties to whom the personal information was sold or shared; and
3. the categories of personal information that the business disclosed about the consumer for a business purpose and the categories of persons to whom it was disclosed for a business purpose.

Verifiable Consumer Requests

A business must only provide this information upon receipt of a "Verifiable Consumer Request" ("VCR"), which is a request that permits the business to reasonably verify that the individual making the request is the consumer, or an individual authorized to act on behalf of the consumer, about whom the business has collected personal information.

A business must make available to consumers two (2) or more designated methods for submitting requests, including, at a minimum, a toll-free telephone number; and if a business maintains an internet website, it must make the internet website available to consumers to submit requests. However, a business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information is only required to provide an email address for submitting requests.

Responding to a Verifiable Consumer Request

Timeframe for Response

A business is required to disclose and deliver the required information to a consumer, free of charge, within forty-five (45) days of receiving a VCR from the consumer. This time period may be extended once by an additional forty-five (45) days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period.

Delivery Method

A business's disclosure of the required information must be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, "in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance." Although a business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, it must not require the consumer to create an account with the business in order to make a VCR. However, in the event the consumer has an existing account with the business, the business may require the consumer to use that account to submit a VCR.

Applicable Time Period

The information provided must cover the 12-month period preceding the business' receipt of the VCR. A consumer may request that the business disclose the required information beyond the 12-month period (limited to personal information collected on or after January 1, 2022), and the business is required to provide that information unless doing so proves impossible or would involve a disproportionate effort. There is no obligation to provide this information to the same consumer more than twice in a 12-month period.

Individual Rights: *Right to Request Deletion of Personal Information Collected From Consumer*

A consumer has the right to request that a business delete any personal information about the consumer that the business has collected from the consumer. A business must inform consumers of their right to request the deletion of their personal information.

Deletion is not required where the personal information is necessary to:

- complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated by the consumer within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer;
- help to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for those purposes;
- debug to identify and repair errors that impair existing intended functionality;
- exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law;
- comply with the California Electronic Communications Privacy Act;
- engage in public or peer-reviewed scientific, historical, or statistical research that conforms or adheres to all other applicable ethics and privacy laws, when the business's deletion of the information is likely to render impossible or seriously impair the ability to complete such research, if the consumer has provided informed consent;
- undertake internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business and compatible with the context in which the consumer provided the information; and
- comply with a legal obligation.

Verifiable Consumer Requests

A business must only provide this information upon receipt of a "Verifiable Consumer Request" ("VCR"), which is a request that permits the business to reasonably verify that the individual making the request is the consumer, or an individual authorized to act on behalf of the consumer, about whom the business has collected personal information.

A business must make available to consumers two (2) or more designated methods for submitting requests, including, at a minimum, a toll-free telephone number; and if a business maintains an internet website, it must make the internet website available to consumers to submit requests. However, a business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information is only required to provide an email address for submitting requests.

Responding to a Verifiable Consumer Request

Timeframe for Response

A business that receives a VCR from a consumer to delete the consumer's personal information must delete the consumer's personal information from its records, notify any Service Providers or Contractors to delete the consumer's personal information from their records, and notify all Third Parties to whom the business has sold or shared the personal information to delete the consumer's personal information unless this proves impossible, involves disproportionate effort, or the personal information is subject to an exception set forth above.

A business is required to delete the personal information, free of charge, within forty-five (45) days of receiving a VCR from the consumer. This time period may be extended once by an additional forty-five (45) days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period.

Delivery Method

A business's disclosure of the required information must be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, "in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance." Although a business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, it must not require the consumer to create an account with the business in order to make a VCR. However, in the event the consumer has an existing account with the business, the business may require the consumer to use that account to submit a VCR.

Individual Rights: *Limit Use and Disclosure of Sensitive Personal Information*

A consumer has the right, at any time, to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, or as otherwise permitted under the CPRA.

A business that uses or discloses a consumer's sensitive personal information for purposes other than those permitted under the CPRA must provide notice to consumers that this information may be used, or disclosed to a Service Provider or Contractor, for additional, specified purposes and that consumers have the right to limit the use or disclosure of their sensitive personal information.

Note: Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to these requirements.

Definition of Sensitive Personal Information

The CPRA defines "Sensitive Personal Information" as:

1. the processing of biometric information for the purpose of uniquely identifying a consumer;
2. personal information collected and analyzed concerning a consumer's health;
3. personal information collected and analyzed concerning a consumer's sex life or sexual orientation; and
4. personal Information that reveals:

    a. a consumer's social security, driver's license, state identification card, or passport number;
    b. 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;
    c. a consumer's precise geolocation;
    d. a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;
    e. the contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication; or
    f. a consumer's genetic data.

How to Request Limitation on Use or Disclosure

A business that discloses consumers' sensitive personal information for purposes other than those authorized by the CPRA must either:

1. provide a clear and conspicuous link on the business's internet homepages, titled "Limit the Use of My Sensitive Personal Information," that enables a consumer, or a person authorized by the consumer, to limit the use or disclosure of the consumer's sensitive personal information to those uses authorized by the CPRA; or

2. allow consumers to limit the use of their sensitive personal information through an opt-out preference signal sent with the consumer's consent to the business indicating the consumer's intent to limit the use or disclosure of the consumer's sensitive personal information.

Note: In lieu of complying with #1 above, a business may choose to utilize a single, clearly labeled link on the business's internet homepages that allows a consumer to opt out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information.

Required Waiting Period Prior to Additional Requests

If a consumer decides to limit the use or disclosure of the consumer's sensitive personal information, the business must wait for at least twelve (12) months before requesting that the consumer authorize the use and disclosure of the consumer's sensitive personal information for additional purposes.

Individual Rights: *Opt Out of Sale or Sharing of Personal Information*

A consumer has the right, at any time, to direct a business that sells or shares personal information about the consumer to Third Parties not to sell or share the consumer's personal information.

A business that sells consumers' personal information to, or shares it with, Third Parties must inform consumers of their right to opt out of the sale or sharing of their personal information.

Age Restrictions

A business is prohibited from selling or sharing the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale or sharing of the consumer's personal information.

Opt-out Mechanisms

A business that sells or shares consumers' personal information must either:

1. provide a clear and conspicuous link on the business's internet homepages, titled "Do Not Sell or Share My Personal Information," to an internet web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale or sharing of the consumer's personal information; or

2. allow consumers to opt out of the sale or sharing of their personal information through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism to the business indicating the consumer's intent to opt out of the business' sale or sharing of the consumer's personal information.

Note: In lieu of complying with #1 above, a business may choose to utilize a single, clearly labeled link on the business's internet homepages that allows a consumer to opt out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information.

Required Waiting Period Prior to Additional Requests

If a consumer opts out of the sale or sharing of personal information, the business must wait for at least twelve (12) months before requesting that the consumer authorize the sale or sharing of the consumer's personal information for additional purposes.

Individual Rights: *Correct Inaccurate Personal Information*

A consumer has the right to request a business that maintains inaccurate personal information about the consumer to correct that inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information.

A business that collects personal information about consumers must disclose the consumer's right to request correction of inaccurate personal information.

Verifiable Consumer Requests

A business must only provide this information upon receipt of a "Verifiable Consumer Request" ("VCR"), which is a request that permits the business to reasonably verify that the individual making the request is the consumer, or an individual authorized to act on behalf of the consumer, about whom the business has collected personal information.

A business must make available to consumers two (2) or more designated methods for submitting requests, including, at a minimum, a toll-free telephone number; and if a business maintains an internet website, it must make the internet website available to consumers to submit requests. However, a business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information is only required to provide an email address for submitting requests.

Business Responses to Verifiable Consumer Requests

Timeframe for Response

A business that receives a VCR to correct inaccurate personal information must use commercially reasonable efforts to correct the inaccurate personal information as directed by the consumer.

A business is required to correct inaccurate personal information, free of charge, within forty-five (45) days of receiving a VCR from the consumer. This time period may be extended once by an additional forty-five (45) days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period.

Individual Rights: *Right to Nondiscrimination*

A business must not discriminate against a consumer because the consumer exercised any of the consumer's rights under the CPRA. Examples of discriminatory acts include:

1. denying goods or services to the consumer;
2. charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;
3. providing a different level or quality of goods or services to the consumer;
4. suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services; and
5. retaliating against an employee, applicant for employment, or independent contractor for exercising their rights under the CPRA.

However, a few exceptions apply to this right, below:

1. A business may charge a consumer a different price or rate, or provide a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.
2. A business may offer loyalty, rewards, premium features, discounts, or club card programs consistent with the CPRA.
3. A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale or sharing of personal information, or the retention of personal information, so long as the consumer provides the business prior opt-in consent that may be revoked at any time.

Obligations if Personal Information Is Provided to a Service Provider, Contractor or Other Third Party

Contractors

The CPRA definition of "Contractor" sets forth specific requirements regarding the contract between the parties. Specifically, "Contractor" means a person to whom the business provides personal information for a business purpose, pursuant to a written contract between the parties that:

- prohibits the Contractor from:

  a. selling or sharing the personal information;
  b. retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract, or as otherwise permitted by the CPRA;
  c. retaining, using, or disclosing the information outside of the direct business relationship between the Contractor and the business; and
  d. combining the personal information that the Contractor receives pursuant to a written contract with the business with personal information that it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, provided that the Contractor may combine personal information to perform a business purpose in limited circumstances;

- includes a certification made by the Contractor that the Contractor understands the restrictions set forth above and will comply with them; and

- permits, subject to agreement with the Contractor, the business to monitor the Contractor's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every twelve (12) months.

Note: Before a Contractor engages any other person to assist it in processing personal information for a business purpose on behalf of the business (or any other person engaged by the Contractor engages another person to assist in processing personal information for that business purpose), the Contractor must notify the business of that engagement, and the engagement must be pursuant to a written contract binding the other person to observe all the requirements set forth above.

Service Providers

Similar to the definition of "Contractor," the CPRA definition of "Service Provider" sets forth specific requirements regarding the contract between the parties. Specifically, "Service Provider" means a person that processes personal information on behalf of a business and that receives from or on behalf of the business personal information for a business purpose pursuant to a written contract between the parties that prohibits the Service Provider from:

- selling or sharing the personal information;

- retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract, or as otherwise permitted by the CPRA;

- retaining, using, or disclosing the information outside of the direct business relationship between the Service Provider and the business; and

- combining the personal information that the Service Provider receives from, or on behalf of, the business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that the Service Provider may combine personal information to perform a business purpose in limited circumstances.

The contract may also, subject to agreement with the Service Provider, permit the business to monitor the Service Provider's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every twelve (12) months.

Note: Before a Service Provider engages any other person to assist it in processing personal information for a business purpose on behalf of the business (or any other person engaged by the Service Provider engages another person to assist in processing personal information for that business purpose), the Service Provider must notify the business of that engagement, and the engagement must be pursuant to a written contract binding the other person to observe all the requirements set forth above.

Third Parties

The CPRA defines "Third Party" as a catchall category for other persons that may receive personal information. Specifically, the CPRA defines a "Third Party" as a person who is not any of the following:

1. 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 under the CPRA;

2. a Service Provider to the business; or

3. a Contractor.

Required Contract Elements for Disclosures to Service Providers, Contractors, or Other Third Parties

In addition to any applicable contract elements discussed above, before a business may sell or share personal information with a Third Party, or disclose personal information to a Service Provider or Contractor for a business purpose, the business must enter into an agreement with the Third Party, Service Provider, or Contractor, that:

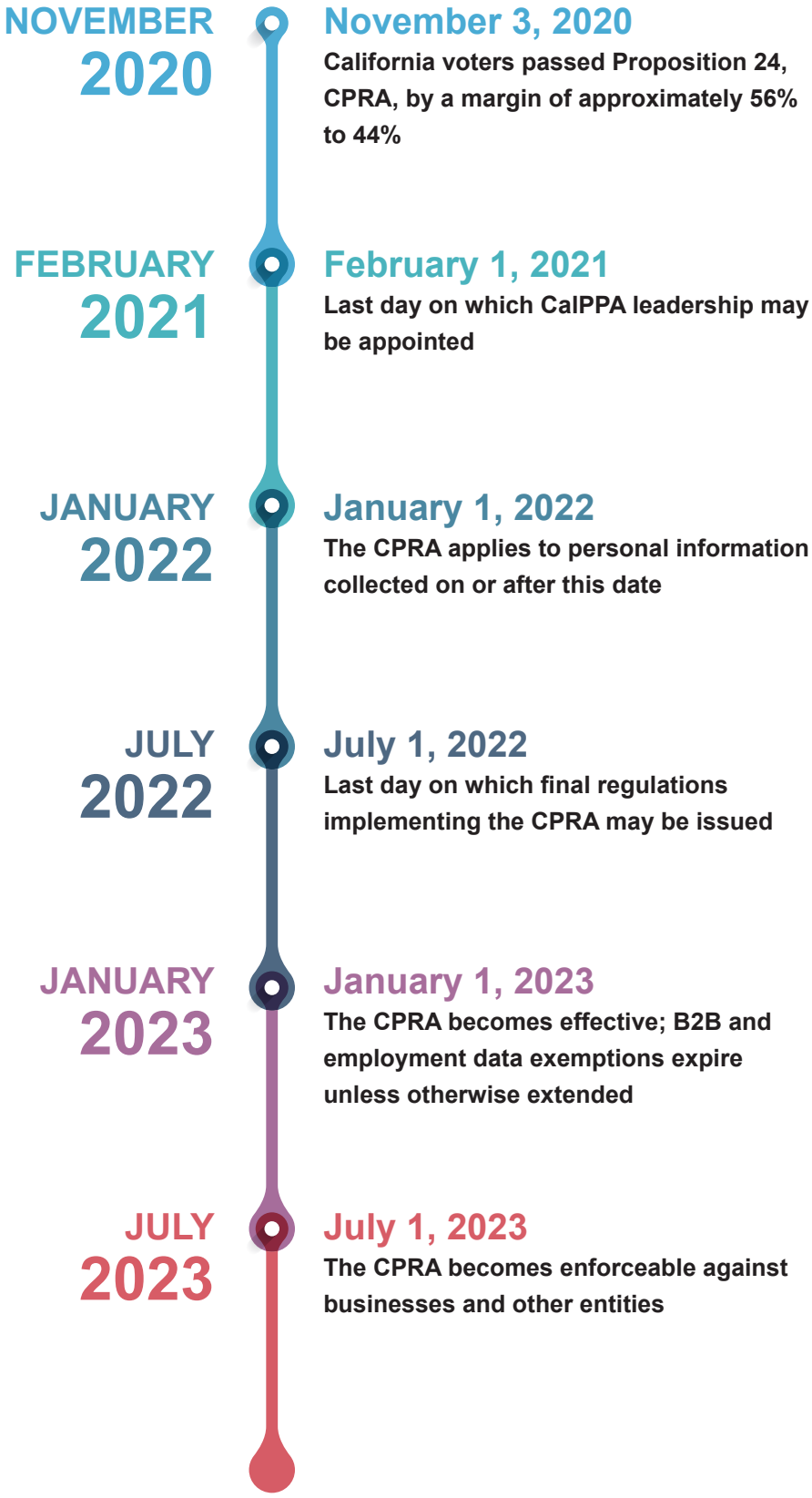
- specifies that the personal information is sold or disclosed by the business only for limited and specified purposes;
- obligates the Third Party, Service Provider, or Contractor to comply with applicable obligations under the CPRA and obligates those persons to provide the same level of privacy protection as is required by the CPRA;
- grants the business rights to take reasonable and appropriate steps to help ensure that the Third Party, Service Provider, or Contractor uses the personal information transferred in a manner consistent with the business's obligations under the CPRA;
- requires the Third Party, Service Provider, or Contractor to notify the business if it makes a determination that it can no longer meet its obligations under the CPRA; and
- grants the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

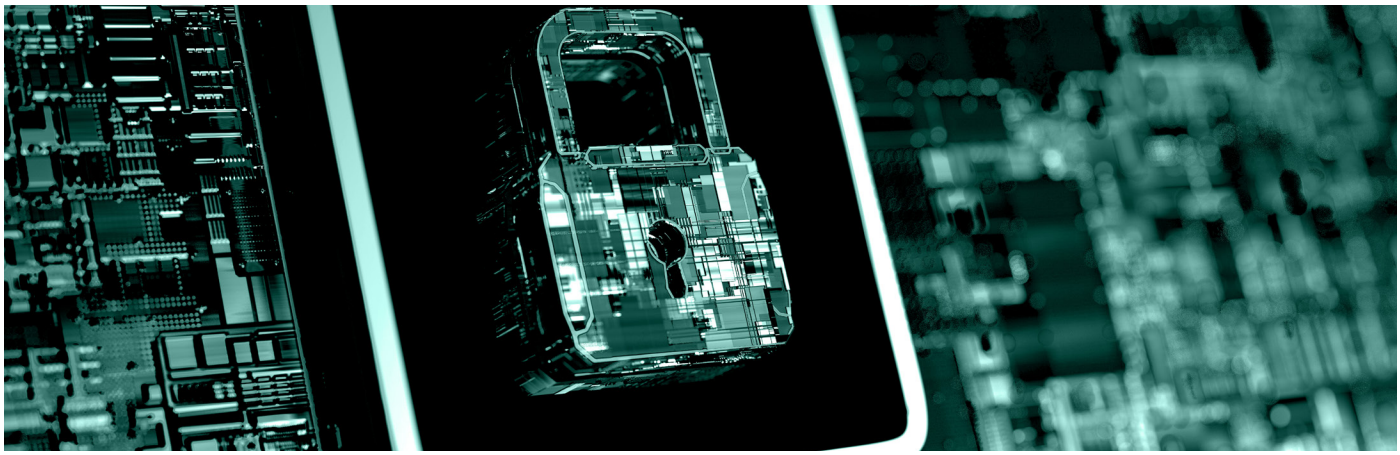
Enforcement and Liability

The CPRA increases both enforcement and potential penalties businesses may face.

The CPRA transfers authority to pursue violations from the California Attorney General to a new privacy-focused agency, the California Privacy Protection Agency (CalPPA). When facing an enforcement action, businesses will no longer have CCPA's 30-day cure period before being fined for a violation by CalPPA. In addition, the CPRA introduces an automatic $7,500 fine for a violation involving the personal information of minors.

In addition to consumers' existing private right of action for breaches of unredacted and unencrypted personal information, the CPRA makes a private right of action available if an email address and password or security question and answer that would allow access to the account is breached.


NOVEMBER 2020
November 3, 2020
California voters passed Proposition 24, CPRA, by a margin of approximately 56% to 44%
FEBRUARY 2021
February 1, 2021
Last day on which CalPPA leadership may be appointed
JANUARY 2022
January 1, 2022
The CPRA applies to personal information collected on or after this date
JULY 2022
July 1, 2022
Last day on which final regulations implementing the CPRA may be issued
JANUARY 2023
January 1, 2023
The CPRA becomes effective; B2B and employment data exemptions expire unless otherwise extended
JULY 2023
July 1, 2023
The CPRA becomes enforceable against businesses and other entities



Compliance Checklist

- [ ] Evaluate whether your business is subject to the CPRA
- [ ] Use the CPRA as an opportunity to review and refresh your CCPA compliance program
- [ ] Update your personal data inventory
- [ ] Determine if you collect “Sensitive Personal Information”
- [ ] Establish a process to implement the right to correct personal information
- [ ] If applicable, establish a process to implement the right to limit use and disclosure of sensitive personal information
- [ ] Address compliance obligations for your “contractors”
- [ ] Determine if and how CPRA’s sell/share distinction affects your organization
- [ ] Address CPRA’s collection, use and retention limitations
- [ ] Analyze whether your business engages in “profiling”
- [ ] Determine if your business is subject to new risk assessment and audit requirements for high-risk businesses
- [ ] Update your current privacy training programs
- [ ] Keep abreast of new regulations and guidance

About Shipman

Shipman's value lies in our commitment -- to our clients, to the profession and to the community.

We have one goal: to help our clients achieve their goals. How we accomplish it is simple: we devote our considerable experience and depth of knowledge to understand each client's unique needs, business and industry, and then we develop solutions to meet those needs.

Clients turn to us when they need a trusted advisor. With our invaluable awareness of each client's challenges, we can counsel them at every step -- to keep their operations running smoothly, help them navigate complex business transactions, position them for future growth, or resolve business disputes. The success of our clients is of primary importance to us and our attorneys invest meaningful time getting to know the client's business and are skilled in the practice areas and industry sectors critical to that success.

With more than 150 lawyers in offices throughout Connecticut, New York and in Washington, DC, we serve the needs of local, regional, national and international clients. Our clients include public and private companies, institutions, government entities, non-profit organizations and individuals.

About the Data Privacy and Protection Practice

The Team

Shipman's Data Privacy and Protection practice holds a unique position among mid-size law firms. With four attorneys holding privacy certifications from the International Association of Privacy Professionals, supported by a team of attorneys with in-depth experience in the privacy issues facing specific sectors (health care, education, human resources and more), we provide a special combination of depth, national experience, and accessibility.

Our dynamic and diverse team guides clients across sectors and jurisdictions through each step of the data privacy and protection lifecycle — from initial information collection, management, protection and disposal, and regulatory compliance to post-breach responses, notifications and litigation. Our practice is national; we represent clients across the United States — from New England to Silicon Valley — as well as multinational corporations with a truly global footprint.

Global Reach

Data privacy is a global issue and we offer our clients a worldwide reach through our membership in Interlaw, an international network of law firms in over 80 countries and 140 key cities around the world. This provides our clients access to leading data privacy attorneys worldwide who understand their local markets, all through a seamless and personal engagement with Shipman. Our clients know that they have one team dedicated to their needs and located wherever business takes them.

Contact:

William J. Roberts, FIP, CIPP/US, CIPM

(860) 251-5051
wroberts@goodwin.com

Stephanie M. Gomes-Ganhão, CIPP/US

(860) 251-5239
sgomesganhao@goodwin.com