Skadden

California Consumer Privacy Act: A Compliance Guide

March 2019

Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates

The Americas
Boston
Chicago
Houston
Los Angeles
New York
Palo Alto
São Paulo
Toronto
Washington, D.C.
Wilmington

Europe
Brussels
Frankfurt
London
Moscow
Munich
Paris

Asia Pacific
Beijing
Hong Kong
Seoul
Shanghai
Singapore
Tokyo

Overview

In June 2018, California enacted the California Consumer Privacy Act (CCPA or the Act), which constitutes the broadest and most comprehensive privacy law in the United States to date. The CCPA goes into effect January 1, 2020.

The CCPA will affect any business collecting or storing data about California residents and may effectively set the floor for nationwide privacy protection, since most businesses will not want to maintain two privacy frameworks — one for California consumers and one for all other individuals. In general, the CCPA gives California more information and control over how their personal information is being used, and requires businesses to be more transparent in their handling of that information.

The California Legislature passed the CCPA fairly quickly to avert a proposed ballot initiative in November 2018 that sought to impose even more stringent privacy regulations. The rush to pre-empt the ballot initiative left the CCPA with unintended ambiguities that will need to be resolved over time. This is in addition to the CCPA requirement that the state attorney general develop further guidance in certain key areas. To that end, the attorney general has already begun holding a series of public forums to solicit input. As California's 2018 legislative session drew to a close, the state passed its first amendment to the CCPA. In addition to clarifying some points in the law, the amendment delayed the requirement for the California attorney general to adopt implementing regulations, from January 1, 2020, to July 1, 2020. Enforcement actions may not be brought by the attorney general under the CCPA until the earlier of July 1, 2020, or six months after the publication of final regulations.

Implementing a data privacy compliance program can be a resource-intensive and time-consuming exercise.

Given the CCPA's ambiguities and that the law is not effective until January 1, 2020, with any enforcement actions likely delayed until a few months after that, it may be tempting for companies to put off developing compliance programs and procedures until late 2019. However, as companies learned when seeking to come into compliance with the European Union's General Data Protection Regulation (GDPR), implementing a data privacy compliance program can be a resource-intensive and time-consuming exercise, especially for businesses with

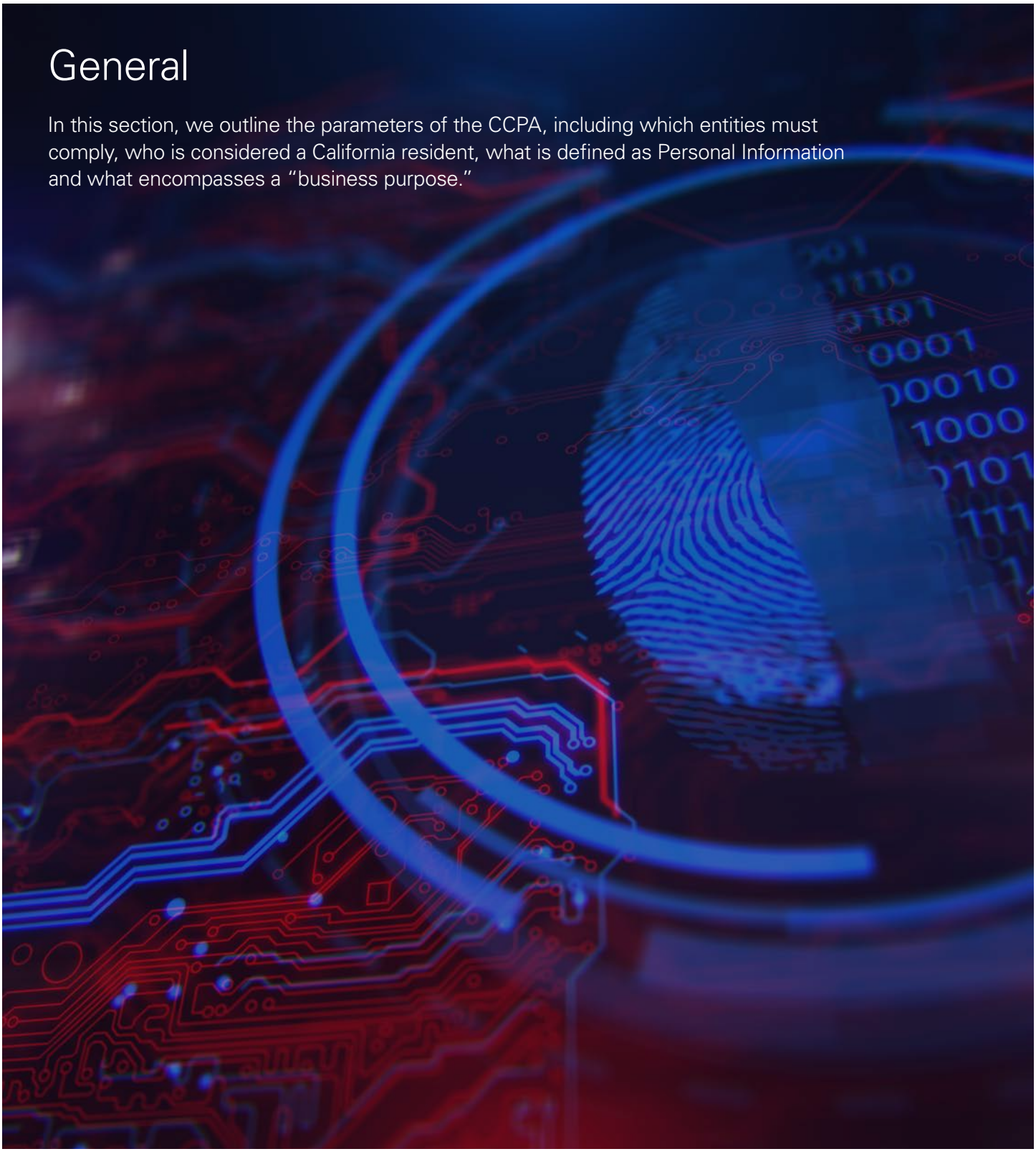
decentralized methods for handling personal information. For companies that have gone through a GDPR compliance program, certain processes and procedures that were developed will have applicability to the CCPA. However, there is no one-to-one match correlation between the GDPR and the CCPA. While in many cases the GDPR imposes more onerous requirements, the CCPA has some unique requirements and also defines personal information more broadly.

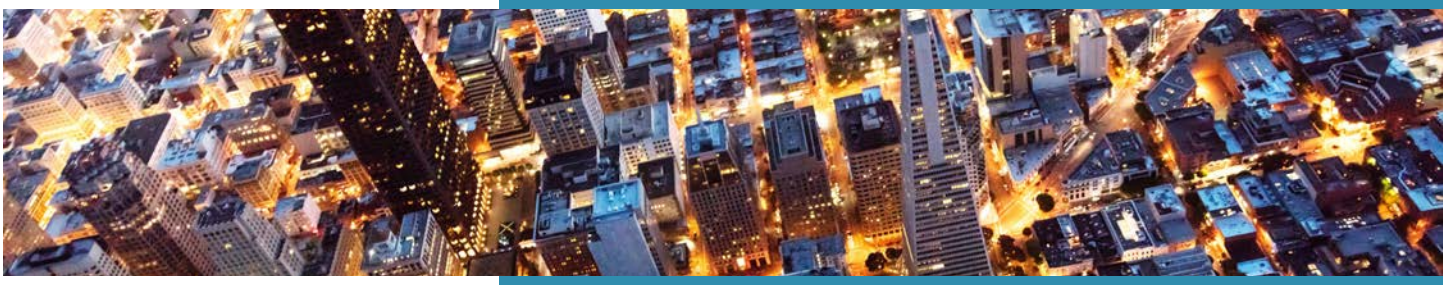
In this CCPA compliance guide, we set forth steps that companies should be taking throughout 2019 to prepare for the CCPA. Although there are, as noted, ambiguities that need to be clarified and guidance to be issued by the attorney general, the steps outlined in this guide will be relevant regardless of any incremental changes to the CCPA in 2019.

Finally, while this guide will be a useful tool for businesses, there can be no substitution for examining the wording of the CCPA itself, including the definitions, since many key provisions are embodied within the defined terms.

General

In this section, we outline the parameters of the CCPA, including which entities must comply, who is considered a California resident, what is defined as Personal Information and what encompasses a "business purpose."





Which Entities Need to Comply With the CCPA?

The CCPA applies to any for-profit entity that (i) does business in California, (ii) collects personal information of California residents (or has such information collected on its behalf), (iii) determines on its own or jointly with others the purpose and means of processing that information, and (iv) meets one or more of the following criteria:

- has annual gross revenues in excess of $25 million, adjusted for inflation;
- annually buys, receives for a commercial purpose, sells or shares the personal information of 50,000 or more consumers, households or devices; or
- derives 50 percent or more of its annual revenues from selling consumers' personal information.

In this guide, we refer to an entity that meet the foregoing criteria as a "Business," which is the term used in the CCPA.

The CCPA defines doing business in California broadly. Indeed, the sole exception is a case where "every aspect" of commercial conduct "takes place wholly outside of California."[1] For example, if a California resident provided information while visiting a retail store in Florida that does not conduct business in California, the CCPA would not apply to that transaction unless the Florida business proceeded to sell that information in California.

Note that the territorial reach of the CCPA is different from the approach used by the GDPR. For example, a California-based business that processes data for customers located in another country would not need to comply with the CCPA with respect to such customer data simply because the company is located in California.

[1] 1798.145(6).

Who Is a California Resident?

A California resident, referred to as a "Consumer" in the CCPA, is anyone who meets the definition of "resident" as defined under the California tax provisions.[2] While the CCPA uses the term "Consumer," Businesses should assume that employees are also swept up in the CCPA's requirements.

In general, the California tax provision defines a California resident as (i) every individual who is in California for other than a temporary or transitory purpose, and (ii) every individual who is domiciled in California but is outside California for a temporary or transitory purpose. Given this second prong, dividing a Consumer base between those who logged into a site from a computer in California and those who did not is not sufficient.

Whether or not a purpose should be considered "temporary or transitory in character" largely depends "upon the facts and circumstances of each particular case." Given the effort required to determine if a Consumer is only temporarily in or out of California, Businesses will likely adopt a broad approach to who is a Consumer.

[2] Section 17014 of Title 18 of the California Code of Regulations.

What Is Personal Information?

Perhaps the most important definition in the CCPA is that of "Personal Information," since all of the CCPA requirements emanate from whether a Business is collecting or processing such information. The CCPA definition is very broad, surpassing in some respects what is covered by the GDPR. Given its importance, we have replicated the CCPA definition below, folding in cross-references where applicable. Note that the list of categories is not exhaustive and that any one "match" satisfies the definition. For example, an email address that includes a full name and a company name (*e.g.*, John.Doe@Acme.com) could be personal information on its own.

> Personal Information means information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household.

Personal Information includes, but is not limited to, the following if it identifies, relates to, describes, is 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.

  Compliance Guide Note: A "unique personal identifier" 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; customer number, unique pseudonym or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. "Family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody. "Device" means any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device.

- ✓ 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.

  Compliance Guide Note:

  - The foregoing categories of Personal Information are those described in subdivision (e) of Section 1798.80 (which deals with Personal Information that is no longer required and should be destroyed) and that do not otherwise overlap with the CCPA.
  - "Health insurance information" is defined as a Consumer's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the Consumer or any information in the Consumer's application and claims history, including any appeals records if the information is linked or reasonably linkable to a Consumer or household (including via a device, by a Business or by a service provider).

- ✓ 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.

  Compliance Guide Note: "Biometric information" is defined as an individual's physiological, biological or behavioral characteristics, including an individual's DNA, that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns and voice recordings, from which an identifier template, such as a faceprint, a minutiae template or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health or exercise data that contain identifying 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, app or advertisement.
- ✓ 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 Educational Rights and Privacy Act.[3]

[3] 20 U.S.C. Section 1232g, 34 C.F.R. Part 99.

- 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.

Note that while the concept of "household" is included in certain categories of Personal Information, that term is itself not defined. It remains unclear whether, for example, two unrelated individuals sharing an apartment would be deemed a "household." We expect further guidance from the attorney general as to how this term is to be understood.

Exceptions to the Personal Information Definition

Information that is publicly available (*i.e.*, lawfully made available from federal, state or local government records) is not covered by the CCPA provided the use is compatible with the purpose for which the data is maintained and made available in the government records. Biometric information collected about a Consumer without the Consumer's knowledge is not deemed "publicly available."

An important exception to the definition of Personal Information is information that is deidentified or part of aggregate consumer information.

- "**Deidentified**" means information that cannot reasonably identify, relate to, describe, be capable of being associated with or be linked, directly or indirectly, to a particular Consumer, provided that a Business that uses deidentified information (i) has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain, (ii) has implemented business processes that specifically prohibit reidentification of the information, (iii) has implemented business processes to prevent inadvertent release of deidentified information, and (iv) makes no attempt to reidentify the information. The challenge for many Businesses will be determining whether information cannot reasonably "be capable of" being associated with a particular Consumer, directly or indirectly, particularly at a time when advances in data analytics are making it easier to recreate an individual's identity from disparate data elements.
- "**Aggregate consumer information**" is defined as information that relates to a group or category of Consumers, from which individual Consumer identities have been removed, and that is not linked or reasonably linkable to any Consumer or household, including via a device.

What Does It Mean to 'Collect' and 'Sell' Personal Information?

Whether or not information has been "collected" triggers a number of CCPA requirements. Here, too, the CCPA adopts a broad definition.

Collection is defined as "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a Consumer by any means." Collecting also includes receiving information from a Consumer "either actively or passively, or by observing the consumer's behavior."

A "sale" of Personal Information under the CCPA is defined broadly to include the "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means" the Personal Information of a Consumer to another business or third party "for monetary or other valuable consideration."

This broad definition suggests that if Personal Information is provided as part of a larger business relationship, a "sale" may have occurred even if no amounts are paid directly for the data itself. In addition, a website may be "selling" Personal Information by passing such information to third-party ad networks through cookies.

The CCPA enumerates certain exceptions to what would be deemed a sale, including when:

- ✓ a Consumer uses or directs the Business to intentionally disclose Personal Information to a third party. An "intentional" interaction occurs when the Consumer intends to interact with the third party via one or more deliberate actions. Hovering over a piece of content or closing it does not qualify as a "deliberate action";
- ✓ a Business shares a Consumer identifier to alert a third party of a Consumer's opt-out decision;

- ☑ Personal Information is shared with a third party to perform a "business purpose" (explained below) and:
  - the Business has provided notice of this sharing and the opt-out right (as described below); and
  - the third party does not further collect, sell or use the Personal Information except as necessary to perform the business purpose;
- ☑ the Personal Information is 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 the Business complies with the CCPA disclosure requirements relating to the disclosure of information collected or sold (discussed below). If the acquirer plans to alter how it will use or share the Personal Information in a manner materially inconsistent with the promises made at the time of collection, it must provide prior notice of the new practices to the Consumer and include a "prominent and robust" notice so the Consumer can opt out. Note that the CCPA also warns Businesses that material, retroactive privacy policy changes must not violate California's Unfair Competition Law — a statement apparently designed to address Businesses that want to make significant changes to a privacy policy in light of an impending deal.

Required Training

A Business is required to ensure that individuals responsible for handling Consumer inquiries about the Business' privacy practices or CCPA compliance are informed about the requirements below, and how to direct Consumers to exercise these rights.

A Business should establish a documented training program to satisfy this requirement:

- ✓ Ensure designated personnel understand how to instruct Consumers to exercise their rights under the CCPA related to:
  - disclosure of Personal Information collected by the Business;
  - disclosure of Personal Information sold by the Business; and
  - opting out of the sale of their Personal Information.
- ✓ Ensure designated personnel understand the general CCPA obligations of the business related to:
  - nondiscrimination related to Consumers who exercise their CCPA rights;
  - "- disclosure obligations of the business, including duties to make available two or more methods for Consumers to make requests, deliver the required information to a Consumer within 45 days (and when an extension exception may apply), confirm a Verifiable Consumer Request (defined on page 22), and identify by category the Personal Information collected, sold or disclosed about the Consumer for a business purpose in the preceding 12 months; and
  - general CCPA compliance obligations of the business, including duties to: provide a clear and conspicuous opt-out link; provide a description of Consumer opt-out rights; effectuate and comply with opt-out requests in business systems; respect opt-out requests for 12 months before requesting that the Consumer authorize a sale; and permit a designated person to opt out on the Consumer's behalf.

Summary of Information to Be Included in Privacy Policies

Under the CCPA, certain information needs to be included in a Business' privacy policy and in any California-specific description of consumers' privacy rights. If a Business does not maintain such policies, this information needs to be included somewhere on its website. Note that this information must be updated at least once every 12 months. The following is required:

- ✓ one or more designated methods for submitting requests permitted under the CCPA;
- ✓ a description of a Consumer's rights to:
  - request disclosure of information collected;
  - request disclosure of information sold;
  - nondiscrimination relating to Consumers who exercise CCPA rights; and
  - opt out, along with a separate link to the "Do Not Sell My Personal Information" opt-out page;
- ✓ a list of the categories (by reference to the CCPA enumerated category) of Personal Information the Business has collected about Consumers in the preceding 12 months; and
- ✓ two separate lists of categories (by reference to the CCPA enumerated category) of information the Business has (i) sold or (ii) disclosed for a business purpose, each within the preceding 12 months or, if the Business has not done so, disclosing that fact.

The 'Business Purpose' Exception

The CCPA refers a number of times to the idea of a "business purpose." It is important to note that a "business purpose" use is not exempt from CCPA requirements. Such use must still be disclosed to a Consumer upon a valid request and be disclosed in a Business' privacy policy. However, certain CCPA obligations do not apply when Personal Information is disclosed for a business purpose. For example, a Consumer cannot "opt out" of a disclosure done for a business purpose, and the age restrictions discussed below do not apply to such disclosures.

A "business purpose" means the Personal Information is being used for the Business' or a service provider's operational purposes, or other purposes disclosead to the Consumer, where the use is (i) "reasonably necessary and proportionate" to achieve the operational purpose for which it was collected or processed, or (ii) for another operational purpose that is compatible with the context in which it was collected.

The CCPA provides a list of what constitutes a "business purpose." Note that this list does not start with the word "including," suggesting it is exhaustive:

- ✔ auditing related to a current interaction with the Consumer (such as counting ad impressions and verifying positioning and quality of ad impressions);
- ✔ detecting security incidents, protecting against malicious, deceptive, fraudulent or illegal activity, and prosecuting those responsible for that activity;
- ✔ debugging errors that impair functionality;
- ✔ short-term, transient use, provided the Personal Information (i) is not disclosed to another third party, and (ii) is not used to build a profile about a Consumer or alter their individual experience outside the current interaction (for example, the contextual customization of ads);

- ✔ performing services such as maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the Business or service provider;
- ✔ undertaking internal research for technological development and demonstration; and
- ✔ undertaking activities to verify or maintain the quality or safety of, or upgrade or enhance, a Business' service or device.

The Research Exception

A Business may retain Personal Information despite a Consumer's valid deletion request where that action would render impossible or seriously impair research goals. The retained Personal Information must be necessary to engage in public or peer-reviewed scientific, historical or statistical research in the public interest.

For this exception to apply, the business must have initially obtained informed Consumer consent for this purpose, and the research must otherwise comply 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 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;
- made subject to technical safeguards that prohibit reidentification of the Consumer to whom the information may pertain;
- subject to business processes that specifically prohibit reidentification of the information;
- 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;
- not be used for any commercial purpose; and
- subjected by the business conducting the research to additional security controls limiting access to the research data to only those individuals in a business as are necessary to carry out the research purpose.

Exemptions From the CCPA

Although the CCPA contains a number of broad requirements, there are certain exceptions to its application that should be noted. Specifically, the obligations imposed by the CCPA do not restrict a Business' ability to:

- comply with federal, state or local laws;
- comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state or local authorities;
- cooperate with law enforcement agencies concerning conduct or activity that the business, service provider or third party reasonably and in good faith believes may violate federal, state or local law;
- exercise or defend legal claims;
- collect, use, retain, sell or disclose consumer information that is deidentified or aggregate consumer information (see above for how "deidentified" and "aggregate consumer information" are defined); or
- collect or sell a consumer's Personal Information if every aspect of that commercial conduct takes place wholly outside of California.

A Business also does not need to honor a request to disclose information collected or sold where it would violate an evidentiary privilege under California law. A Business can also provide the Personal Information of a Consumer to a person covered by an evidentiary privilege under California law, as part of a privileged communication.

Additionally, the CCPA does not apply to:

- medical information governed by the California 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 established pursuant to the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH);
- 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 it protects medical information or protected health information under HIPAA and HITECH;

- information collected as part of a clinical trial subject to 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 U.S. Food and Drug Administration;
- the sale of Personal Information to or from a consumer reporting agency if the information is to be reported in, or used to generate, a consumer report, and use of that information is limited by the federal Fair Credit Reporting Act;
- personal information that is collected, processed, sold or disclosed pursuant to the federal Gramm-Leach-Bliley Act (GLB) and implementing regulations, or the California Financial Information Privacy Act (FIPA); and
- personal information that is collected, processed, sold or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (DPPA).

Note that the carve-outs for information collection under GLB, FIPA or DPPA do not apply to the right to bring a private action for a data security breach (as described below).

Private Rights of Action and Enforcement by the Attorney General

The CCPA provides for both a limited private right of action for Consumers and more robust enforcement capabilities for the California attorney general.

Private Right of Action

Although there is no broad private right of action for CCPA violations, a Consumer may bring such an action against a Business where the Consumer's nonencrypted or nonredacted personal information is subject to an unauthorized access and exfiltration, theft or disclosure. Significantly, for purposes of this private right of action, personal information is defined using the narrower definition for that term in the California law that deals with securing personal information[4] and not the very broad CCPA definition. Under the narrower definition, personal information is generally limited to name plus Social Security number, driver's license, financial account number (with passcode), medical information and health insurance information.

In order for a private right of action to arise under the CCPA, an incident must result from the Business' failure to implement and maintain "reasonable security procedures and practices appropriate to the nature of that information." Although the CCPA provides no guidance on what would be deemed "reasonable," California law already required reasonable data security measures,[5] and the attorney general's 2016 California Data Breach Report listed 20 data security controls from the Center for Internet Security that serve as a minimum baseline for an information security program. Businesses can assume that these standards would apply equally to the security requirements under the CCPA and should consider them in light of the nature of the Personal Information the Business holds.

A Consumer may recover any of the following through a civil action:

- ✔ statutory damages in an amount of $100 to $750 per consumer per incident, or actual damages (whichever is greater);

[4] Section 1798.81.5.
[5] Section 1798.81.5.

- ✓ injunctive or declaratory relief; and
- ✓ any other relief the court deems proper.

In assessing statutory damages, the CCPA directs a court to consider: (i) the nature and seriousness of the misconduct, (ii) the number of violations, (iii) the persistence of the misconduct, (iv) the length of time over which the misconduct occurred, (v) the willfulness of the defendant's misconduct, and (vi) the defendant's assets, liabilities and net worth.

Prior to filing an action for statutory damages, the Consumer must provide the Business with 30 days' written notice identifying the specific provisions of the CCPA allegedly violated. If the violation is curable, the Business cures the violation within 30 days and provides the Consumer with an express written statement to that effect, and no additional violations have occurred, the Consumer may not initiate an action. However, no such notification is required if the Consumer suffered actual pecuniary damages. If a Business breaches its written statement to the Consumer and continues to violate the CCPA, the Consumer may initiate an action against the Business to enforce the written statement, along with all other remedies under the CCPA. It is important to note that the original draft of the CCPA seemed to allow a private right of action for any violation of the CCPA, in which case this notice provision made sense. However, a subsequent amendment clarified that the only private cause of action is for the security breach described above. It is not clear how this notice and cure provision would apply in the case of a security breach.

This private right of action will go into effect on January 1, 2020. Companies should carefully evaluate their security programs, particularly in light of the 2016 California Data Breach Report; monitor the compliance of their vendors; and consider what personal information is not encrypted or redacted.

Attorney General Enforcement

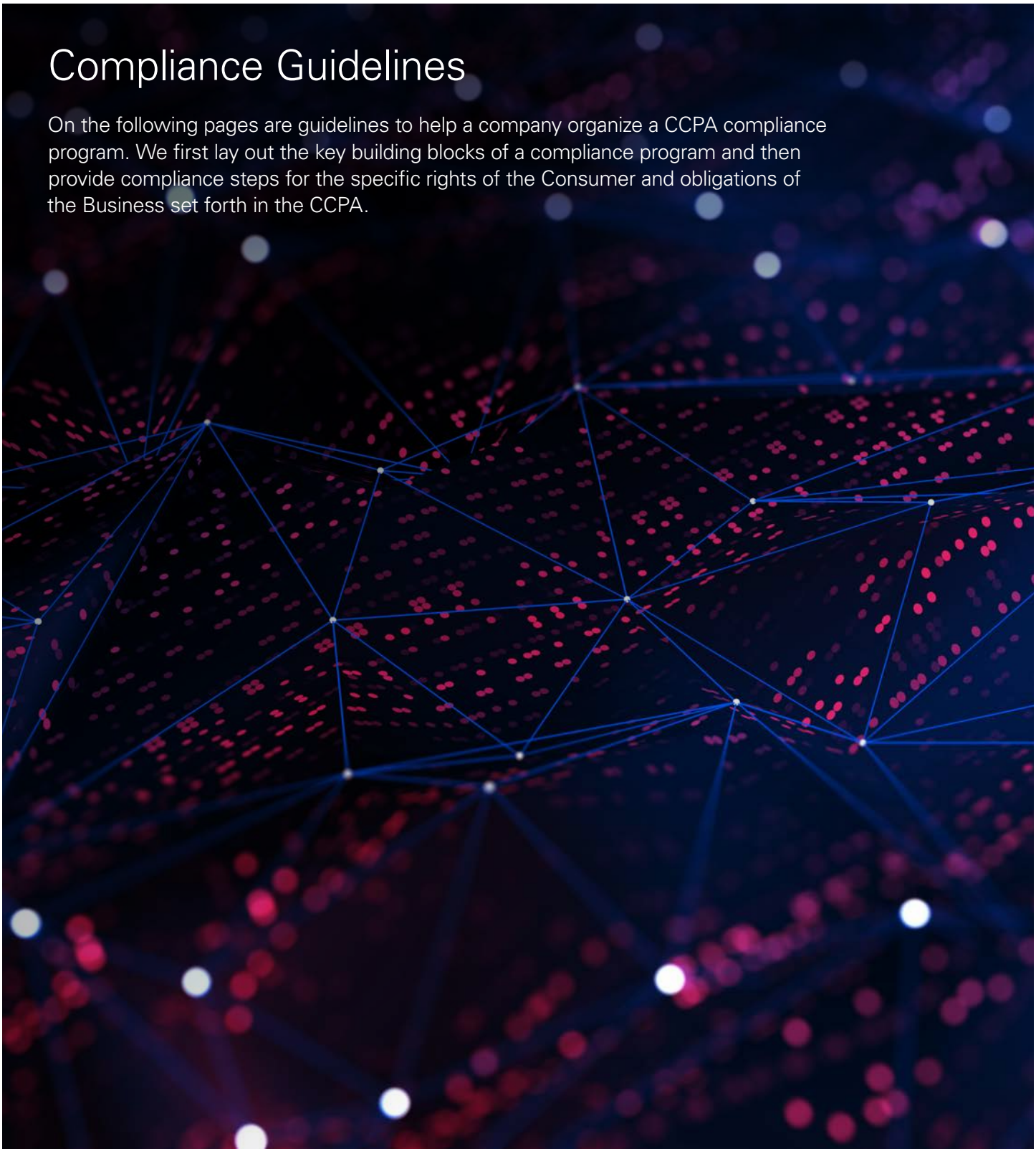
The California attorney general has sole authority to bring civil actions based on general violations of the CCPA requirements. The attorney general is required to give a Business 30 days to cure a violation before an action can be brought. Once this period has passed, if the violation is not cured, the attorney general may seek:

- ✓ an injunction; and
- ✓ a civil penalty of no more than $2,500 for each violation, or $7,500 for each intentional violation of the CCPA.

These funds will be deposited in the newly created Consumer Privacy Fund, which is intended to offset costs incurred by the courts and the attorney general in connection with the CCPA.

Compliance Guidelines

On the following pages are guidelines to help a company organize a CCPA compliance program. We first lay out the key building blocks of a compliance program and then provide compliance steps for the specific rights of the Consumer and obligations of the Business set forth in the CCPA.



General Steps

Create a Data Map

In order to comply with many of the CCPA's requirements, a Business must first have ready access to certain facts about the Personal Information it collects. This includes:

- what Personal Information it has collected about a Consumer (both by "category" and specific information), taking into account the broad definition of "collection" noted above;
- the source of that Personal Information (*e.g.*, did the Business collect it directly or obtain it from a third party);
  - If from a third party, is there an agreement with that party as to Personal Information use or collection?;
- how that Personal Information was collected (*e.g.*, as part of an online application, in the course of a sales transaction, as part of a marketing campaign, etc.);
- where that Personal Information is stored and when it is deleted;
- how Personal Information is used by the Business and who has the authority to determine or change that use;
- what Personal Information, if any, was "sold" to a third party (including the identity of those third parties, the method of "sale" and what rights they were granted in the Personal Information), taking into account the broad definition of a "sale" noted above;
- whether the business knows, or can reasonably ascertain, the age of the Consumer; and
- whether the Consumer has any type of account with the Business.

A best practice to gather and sort this information is by creating a "data map" that traces what Personal Information is ingested by the company and how it is "collected," used, processed, stored and "sold." While there are a variety of ways to organize a data map, most Businesses will find that organizing this information in a way that mirrors how the Businesses itself is organized will capture the necessary data.

Document Processes and Procedures

While the CCPA does not require that a Businesses document its compliance processes and procedures, it is a best practice to do so. Most Businesses will find it challenging to comply with the CCPA's requirements without written policies and procedures in place. In addition, if a Business needs to defend its compliance activities in a litigation or enforcement action, it will be important to have documentation to show the steps the Business takes in general, and how it addressed the specific issue at hand.

Right to Access What Information a Business Has Collected

A Consumer has a right to request disclosure of the categories and specific pieces of Personal Information the Business has collected about the Consumer. The reference to "categories" are those set forth in the definition of Personal Information.

Submission Options: The Business must make available to Consumers two or more designated methods for submitting requests, including, at a minimum, a toll-free telephone number, and if the Business maintains a website, a website address.

Verifiable Consumer Request: Businesses must only provide this information after receipt of a Verifiable Consumer Request (**VCR**).

- A "Verifiable Consumer Request" means a request where a Business can verify that the Consumer making the request is the Consumer about whom the business has collected Personal Information or is a person authorized by the Consumer to act on such Consumer's behalf. The attorney general will need to promulgate guidance on what constitutes a VCR, although the Act suggests that a Business can deem a request from a Consumer who is already logged into a service to be verified.

Response Time: Business must respond to a VCR by mail or electronically within 45 days (which can be extended for an additional 45 days upon notice to the consumer). The Business needs to inform the Consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay. Note: In a different section, the CCPA states the response to any VCR can be extended for an additional 90 days. It is unclear whether this is in addition to the two 45 day periods noted here.

Portability Format: The Personal Information, if provided electronically, should be in a portable and in a readily usable format that allows the consumer to transmit this information from one entity to another entity "without hindrance."

Method to Deliver the Information: If the Consumer has an account with the Business the Personal Information should be delivered through that account. If the Consumer does not have such an account, it can be delivered by mail or electronically at the Consumer's option. Note that a Business cannot require a consumer to create an account in order to submit a VCR.

Applicable Time Period: There is no obligation to provide this information to a Consumer more than twice in a 12-month period, and the information provided need only cover the 12-month period prior to the VCR.

Compliance Recommendations

- ☑ Create and make available to Consumers the Submission Options noted above.
- ☑ Establish a means to establish a request is a proper VCR. As noted, additional guidance is required from the attorney general as to what this will require.
- ☑ Create a process to readily access the specific Personal Information the Business has about each Consumer. This includes knowing what Personal Information is held and what "category" it falls into; where it is stored; and having the ability to extract it.
- ☑ Create a tracking system to ensure compliance with the Response Time and that the request complies with the Applicable Time Period.
- ☑ Create a means to provide requested Personal Information in a portable and readily usable format.
- ☑ Create a tracking system of each access request and how it was handled to be able to demonstrate compliance.

Right to Request Deletion of Information Collected From Consumer

A Consumer has a right to request the Business delete Personal Information that the Business has collected about them. Note that the CCPA does not currently specify what actions are sufficient to constitute "deletion."

Submission Options: The required Submission Options are the same as noted in the "right to access" section above.

Exceptions: Deletion is not required where the Personal Information is necessary to:

- complete the transaction for which the Personal Information was collected; provide a good or service requested by the Consumer or reasonably anticipated within the context of a Business' ongoing relationship with the Consumer; or otherwise perform a contract between the Business and a Consumer;
- detect security incidents, protect against malicious, deceptive, fraudulent or illegal activity, or prosecute those responsible for that activity;
- debug and to identify and repair errors that impair functionality;
- exercise or ensure free speech or other legal rights;
- comply with the California Electronic Communications Privacy Act;
- engage in certain research in the public interest that adheres to all other applicable ethics and privacy laws, when deletion is likely to render impossible or seriously impair such research, if the Consumer has provided informed consent;
- undertake internal uses that are reasonably aligned with the expectations of the Consumer's relationship with the Business;
- comply with a legal obligation; and
- otherwise undertake internal uses in a lawful manner that are compatible with the context in which the Consumer provided the information.

Response Time: The Response Time is the same as noted in the "right to access" section above.

Notification to Service Providers: The Business must also direct any service provider to delete the applicable Personal Information.

Notice to Consumers: The Business must inform Consumers of their right to request the deletion of their Personal Information.

Compliance Recommendations

- ☑ Create and make available to Consumers the Submission Options noted above.
- ☑ Establish a means to determine whether a request is a proper VCR. As noted, additional guidance is required from the attorney general as to what this will require.
- ☑ Create a tracking system to ensure compliance with the Response Time.
- ☑ Establish a process to determine if one of the exceptions to the deletion right noted above applies.
- ☑ Create a process to readily access the specific Personal Information the Business has about each Consumer, and develop a means to delete that Personal Information.
- ☑ Provide notice to the Consumer about the right to request deletion and the process for making a request, either in a privacy policy or on the Business' website.
- ☑ Have the ability to identify service providers who might have received the Personal Information, and develop procedures to effectuate deletion by those providers.
  - Ensure that any agreements with service providers include this obligation.
- ☑ Create a tracking system of each deletion request and how it was handled to be able to demonstrate compliance.

Right to Request Disclosure of Information Collected and Shared

A Consumer who has made a proper VCR has a right to request a Business that has collected Personal Information about the Consumer to provide details relating to certain aspects of the Business' data practices. Specifically, a Consumer can request disclosure of: (i) categories of Personal Information collected about that Consumer in the prior 12 months, (ii) the categories of sources from which the Personal Information is collected, (iii) the business/commercial purpose for collecting and selling Personal Information, (iv) categories of third parties with whom the Business shares Personal Information, and (v) specific pieces of Personal Information collected about the Consumer. Note that the first and last categories overlap with the right to access described above.

Submission Options: The required Submission Options are the same as noted in the "right to access" section above.

Response Time: The Response Time is the same as noted in the "right to access" section above.

Applicable Time Period: The Applicable Time Period is the same as noted in the "right to access" section above.

Notice to Consumers: The Business must provide a list of the categories of Personal Information it has collected about Consumers in the preceding 12 months either within its privacy policy or, if it does not have a privacy policy, on its website. This information needs to be updated once every 12 months.

Limitations: A Business is not required to retain Personal Information about a Consumer collected for a single one-time transaction if that information would not normally be retained. Nor is it required to reidentify data that, in the ordinary course of business, is not maintained in a manner that would be considered Personal Information.

Compliance Recommendations

- ☑ Create and make available to Consumers the Submission Options noted above.
- ☑ Establish a means to determine whether a request is a proper VCR. As noted, additional guidance is required from the attorney general as to what this will require.
- ☑ Create a process to readily access the specific Personal Information the Business has about each Consumer to satisfy this disclosure requirement.
- ☑ Create a tracking system to ensure compliance with the Response Time and that the request complies with the Applicable Time Period.
- ☑ Create and post a list of the categories of Personal Information collected about Consumers in the preceding 12 months either within the Business' privacy policy or, if the Business does not have a privacy policy, on its website. Establish a process to update this information once every 12 months.
- ☑ Create a tracking system of each disclosure request and how it was handled to be able to demonstrate compliance.

Right to Disclosure of Categories of Information Sold

A Consumer who has made a proper VCR has a right to request that a Business that sells the Consumer's Personal Information or discloses it for a business purpose provide an itemized list of the categories of Personal Information (i) collected about the Consumer, (ii) sold about the Consumer (including categories of third parties to whom the information was sold, by category or categories of Personal Information for each third party), and (iii) disclosed about the Consumer for a business purpose. Note the broad definitions of "collected" and "sold" discussed above.

Submission Options: The required Submission Options are the same as noted in the "right to access" section above.

Applicable Time Period: The Applicable Time Period is the same as noted in the "right to access" section above.

Notice to Consumers: Businesses must create and post either within the Business' privacy policy or, if the Business does not have a privacy policy, on its website: (i) a list of the categories of Consumers' Personal Information the Business has sold, or indicate it has not done so, and (ii) a separate list of the categories of Consumers' Personal Information the Business has disclosed for a business purpose, or indicate it has not done so. Establish a process to update this information once every 12 months.

Compliance Recommendations

- ☑ Create and make available to Consumers the Submission Options noted above.
- ☑ Establish a means to determine whether a request is a proper VCR. As noted, additional guidance is required from the attorney general as to what this will require.
- ☑ Create a process to readily access the specific Personal Information the business has collected and sold about each Consumer to satisfy this disclosure requirement.
- ☑ Create a tracking system to ensure compliance with the Response Time and that the request complies with the Applicable Time Period.
- ☑ Create and post in the Business' privacy policy or on the Business' website if it does not have a privacy policy: (i) the categories of Consumers' Personal Information it has sold, or indicate it has not done so, and (ii) the categories of Consumers' Personal Information it has disclosed for a business purpose, or indicate it has not done so. This must be updated at least once every 12 months.

Right to Opt Out of the Sale of Personal Information

A Consumer has a right, at any time, to opt out of the sale of their Personal Information by a Business to third parties. A Consumer can authorize someone to opt out on their behalf, but the means to do this still needs to be specified by the attorney general.

Notice to Consumers:

- The Business must provide, on its homepage, a clear link titled "Do Not Sell My Personal Information," which links to an opt-out page. A Business is permitted to create a separate homepage for California Consumers with this link (and omit it from the general homepage) if it takes reasonable steps to ensure California Consumers are directed to the California homepage.
- The foregoing link and a description of this right must also be disclosed in the Business' privacy policy and any California-specific description of Consumers' privacy rights.

Training: Individuals responsible for handling Consumer privacy inquiries and CCPA compliance must be trained on the opt-out right and how to direct consumers to exercise that right.

Requesting New Consent: If a consumer has opted out, the Business cannot request authorization to sell the Consumer's Personal Information for 12 months.

Use of Opt-Out Request Information: Personal Information collected from the Consumer's opt-out request can only be used to comply with that request.

Application to Third Parties: A third party that has received Personal Information from a Business may not sell that Information unless the Consumer has received explicit notice and an opportunity to opt out.

Age Restrictions:

- A Business with actual knowledge that a Consumer is between 13 and 16 cannot sell that Consumer's Personal Information without affirmative opt-in consent. A Business that willfully disregards a Consumer's age is deemed to have actual knowledge of the Consumer's age. The CCPA does not provide additional guidance on how willful disregard is determined or if knowledge is presumed for sites directed to children.
- A Business with actual knowledge that a Consumer is under age 13 cannot sell that Consumer's Personal Information without affirmative opt-in consent of that Consumer's parent or guardian.

Compliance Recommendations

- ☑ Develop a means of tagging, tracking and separately treating the Personal Information of Consumers who have exercised their opt-out rights.
- ☑ Prominently display the opt-out button on the business website once requirements are released by the attorney general.
- ☑ Determine what Consumer information is necessary to effectuate an opt-out.
- ☑ Develop a process allowing for a parent or guardian to opt in on behalf of a Consumer who falls within the age restrictions.
- ☑ Since a Business that willfully disregards the Consumers' age is deemed to have actual knowledge, Businesses may wish to develop a means of classifying a Consumer based on the Personal Information they have on them.
- ☑ Where a Business has purchased Personal Information, develop a verification mechanism to confirm Consumer notification consent prior to further sale of such data.

Right to Nondiscrimination

Businesses may not discriminate against a Consumer who exercises their rights under the CCPA. Examples of discriminatory actions include: (i) denying goods or services to the Consumer, (ii) charging different prices (including offering discounts to those who do not opt out), (iii) varying the level or quality of goods or services, or (iv) suggesting the Consumer will receive a different price for goods or services, or different level or quality.

Exceptions:

- Businesses can charge different prices, or provide a different level or quality of goods or services, if that difference is reasonably related to the value provided to the Consumer by the Consumer's data.
- Businesses may offer financial incentives for the collection, sale or deletion of Personal Information if the Business has notified the Consumer of the material terms of the incentive and obtained opt-in consent prior to enrollment. The Consumer has the right to withdraw this opt-in at any time.
- Any financial incentive practice cannot be unjust, unreasonable, coercive or usurious in nature.

Compliance Recommendations

- ☑ Note that this requirement does not have a parallel in the GDPR, and therefore even companies fully compliant with the GDPR will need to add processes to comply with it.
- ☑ Businesses should review their business practices as it relates to Personal Information to ensure they are not providing any incentives that would violate the nondiscrimination requirement. They should also put in place policies and procedures to ensure that such practices are not adopted in the future. For example, have all incentive programs relating to Personal Information reviewed by the legal department or a designated committee.
- ☑ If the Business plans to offer a permitted financial incentive for the collection, sale or deletion of Personal Information, ensure that the Consumer was notified of all material terms and direct the Consumer to the Business' opt-in page.
  - Establish a clear process for Consumers to revoke their opt-in decision, and ensure that decision is honored.
- ☑ Develop a means to tag and track users who have opted into financial incentives so their Personal Information can be treated separately compared to ones who have not.

Obligations if Personal Information Is Provided to a Service Provider

Although there is no specific CCPA provision dealing with the disclosure of Personal Information to a service provider, the definition of service provider incorporates certain requirements.

Specifically, by implication, a Business can only provide Personal Information to a service provider if:

- the disclosure is for a business purpose and pursuant to a written contract; and
- the contract prohibits the service provider from retaining, using or disclosing the Personal Information for any purpose other than for the specific purpose of performing the services specified in an agreement, or as otherwise permitted by the CCPA.

A Business that discloses Personal Information to a service provider is not liable under the CCPA if the service provider uses it in violation of the CCPA, provided that at the time of disclosure it does not have actual knowledge, or reason to believe, that the service provider intends to violate the CCPA. Similarly, a service provider is not liable under the CCPA for the obligations of the Business for which it provides services. It is important to note that, in contrast to the GDPR, there is no separate set of standards for service providers as there is for "data processors" under the GDPR.

Compliance Recommendations

- ☑ Track and document any disclosure of Personal Information to a third party, and confirm that all such disclosures are for a business purpose.
- ☑ Ensure that there is a written agreement with each such third party. Note that if a Business and its service provider already have a data processing addendum in place to conform with the requirements imposed under the GDPR, that addendum will likely already satisfy any obligations under the CCPA.
- ☑ Ensure that these written agreements explicitly limit the use of the Personal Information to providing the specified services to the Business.

Right to Refuse a Consumer Request

A Business can refuse a request for the deletion or disclosure of Personal Information in two situations:

- A Business can determine it has a basis not to comply with the Consumer's request provided it promptly informs the Consumer of that decision (and at least within the time periods required under the applicable CCPA provisions). That notice must explain the Business' rationale and any rights the Consumer may have to appeal that decision to the Business. Note that the CCPA does not seem to mandate that the Business provide an appeal right. In order to be able to invoke this exception, a Business should have a documented policy for when they will refuse a Consumer request and a mechanism to inform the Consumer of that decision within the required time frame.
- A Business can determine that a request from a Consumer is "manifestly unfounded or excessive, in particular because of their repetitive character." In such a case, the Business can (i) refuse the request provided it promptly informs the Consumer of that decision (and at least within the time periods required under the applicable CCPA provisions), and (ii) can charge a reasonable fee to comply with the request, based on its costs. Although the Business bears the burden of demonstrating that a request is "manifestly unfounded or excessive," the CCPA offers no guidance on how that decision should be made. In order to be able to invoke this exception, Businesses should have a documented policy to determine when a request is excessive so it is not doing so on an ad hoc basis. The Business should also establish a policy as to whether it will charge for the request or refuse it, and if it does charge, have a method for determining a reasonable fee.

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Daniel Healow
Associate / Palo Alto
650.470.3168
daniel.healow@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP / Four Times Square / New York, NY 10036 / 212.735.3000

525 University Ave. / Palo Alto, CA 94301 / 650.470.4500

skadden.com