# California Consumer Privacy Act Privacy Compliance Roadmap

# California Consumer Privacy Act Privacy Compliance Roadmap

## CCPA BACKGROUND

The California Consumer Privacy Act ("**CCPA**") is one of the most sweeping consumer privacy laws to take effect in the history of the United States. The statute imposes transparency and disclosure obligations on businesses' use, sale, and disclosure of consumer information. Businesses also will need to honor requests from consumers to access their personal information, delete their personal information (though broad exceptions apply), and opt out of the sale of their personal information (the concept of "sale" is very broadly defined). The CCPA went into effect on January 1, 2020 and, as of July 1, 2020 is enforceable by the California Attorney General ("**AG**"). The AG also issued final regulations pursuant to the CCPA in August 2020. The materials included in this CCPA Starter Kit have been drafted with reference to the CCPA and the August 2020 version of the regulations. Ongoing CCPA rulemaking activities may necessitate updates to some of the materials contained herein.

The CCPA aims to protect the information of California "**consumers**," which essentially means individuals who reside in California. Consumers are akin to "**data subjects**" in GDPR parlance. Until January 2023, employees are generally excluded from most CCPA provisions, but still (1) have a right to notice at or before collection as laid out in Section 1798.100(b), and (2) may bring a private right of action for uncured breaches of unencrypted data as provided in Section 1798.150.

The CCPA 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 everything from names and email addresses to location data, browsing and device information, professional or employment-related information, and inferences drawn about other data points to create a profile. In certain circumstances, information covered by other privacy laws or regulations, such as HIPAA or the GLBA, is carved out from the CCPA. If you have questions about these exceptions, please contact your Perkins Coie attorney.

The compliance obligations under the CCPA fall upon any "**business**" that satisfies the statutory definition of the term (essentially, a for-profit entity doing business in California, that meets one of three threshold criteria related to revenue, data collection, or sales of personal information). A business under the CCPA is analogous to the GDPR's "controller" concept; like a controller, a "business" under the CCPA "alone, or jointly with others, determines the purposes and means of processing" a consumer's personal information.

## DEVELOPMENTS IN CALIFORNIA PRIVACY LAW

In November 2020, California voters approved the California Privacy Rights Act ("**CPRA**"), which amends and expands the provisions of the CCPA. The CPRA will become fully operative on January 1, 2023, and a new privacy regulatory agency created by the CPRA will issue regulations under the statute prior to that date. The CPRA extends the CCPA's exemptions for employee data and business contact information until January 1, 2023, at which point such data becomes fully subject to the obligations under the CPRA. These CCPA Starter Kit materials are focused on CCPA compliance and do not yet contemplate the obligations of the CPRA, particularly since those obligations may be significantly refined by the upcoming rulemaking activity. If you have questions about preparing for the CPRA, contact your Perkins Coie attorney.

## PREPARING YOUR CCPA ROADMAP

The following sections summarize your obligations as a business and provide a roadmap to move your company toward CCPA compliance. It provides overviews of the statutory and regulatory obligations, recommends steps to satisfy such obligations, and explains how the resources in this CCPA Starter Kit will help you build your CCPA compliance program.

# California Consumer Privacy Act Privacy Compliance Roadmap

## BUILDING YOUR CCPA COMPLIANCE PROGRAM

### 1. PREPARE OR UPDATE YOUR DATA MAP

**EXPLANATION:** Developing a data map (an accurate and comprehensive record of the types of personal information you collect and how such information is used, shared, stored, retained, and secured) will inform almost every aspect of your CCPA compliance. A data map is not an explicit statutory mandate, but you cannot prepare for the CCPA without developing an accurate and comprehensive record of the types of personal information you collect and how such information is used, shared, stored, retained, and secured. Your data map will be the foundation for your privacy policy disclosures, responses to consumer requests, and adjustments to your agreements with vendors.

Companies take different approaches to completing their data maps. But generally, any such process must start by identifying the teams within your company that collect, use, or share personal information (e-commerce, marketing/advertising, customer service, operations/fulfillment, and IT, for example). Then, determine the appropriate contacts in each team to describe personal information collection, use and sharing practices. Work with these individuals to complete the data map portion for their team (see *Resources* box below). You can ask your colleagues to complete the information in writing or interview them—or a combination of both. The information captured in your data map should reflect the current practices of your company as well as plans for the coming 12 months.

#### CCPA STARTER KIT RESOURCES

- Data Map Template
- Data Map Sample Entries

#### OTHER WAYS PERKINS COIE CAN HELP

Perkins Coie assists clients with all aspects of data mapping. Some clients engage us to provide a training to the individuals who will contribute information to the data map to help socialize the exercise and offer legal reasons for completing it. Others engage us to complete the entire process on their behalf (conducting interviews and completing the data map document itself). Finally, another option is to work with Perkins Coie to analyze the information you learn in the data mapping process, particularly to identify types of data sharing that may risk being classified as CCPA Sales (See #2 below). We bill for these services at our hourly rates.

### 2. UNDERSTAND POTENTIAL CCPA "SALES" OF PERSONAL INFORMATION

**EXPLANATION:** Several obligations under the CCPA hinge on whether your company "sells" personal information, as that term is defined in the CCPA, so it is important to understand whether these obligations may apply to your business. The term "sell" is defined broadly to include "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 another business or a third party for monetary or other valuable consideration." Although many companies may not sell personal information outright, transfers that generate value for your company could be alleged to be "sales" under the CCPA. Some disclosures are carved out from the definition of "sale," provided certain restrictions are met. For example, transfers to service providers and disclosures of personal information made at a consumer's direction do not constitute "sales" under the CCPA. (For guidance about reviewing agreements in light of CCPA "sales" obligations, please see #5 below.)

If your company "sells" personal information, you will need to satisfy several important compliance obligations, including the following:

- Offer a functioning method for individuals over 16 to opt out of these "sales" (users under 16 must opt in, and for users under 13, the parent or legal guardian must opt in).
- Include a clear and conspicuous link on your website homepage and mobile app landing page or download page that reads, "Do Not Sell My Personal Information." This link should direct to a webpage containing a description of the right to opt-out, as well as the other content specified in Section 999.306(c) of the regulations. Alternatively, the business should link to the section of the business's privacy policy containing the same information from the opt-out page noted above.

- Upon receipt of an opt-out request, either cease the information disclosure that constitutes a "sale" with respect to the requesting individual, or direct the entity receiving the information to do so.
- Include information about your company's "sales" practices in your privacy policy (see #3 below).

**CCPA STARTER KIT RESOURCES**

- CCPA Sales Analysis Framework
- Data Map Template
- Consumer Rights Playbook
- Guidelines for Service Provider Agreements

**OTHER WAYS PERKINS COIE CAN HELP**

The "sales" analysis is one of the thorniest issues under the CCPA. As you identify the entities to whom you disclose information as part of your data mapping efforts (see #1 above), Perkins Coie can help you review data-sharing practices and agreements to assess risk related to activities that may be CCPA "sales" and trigger-related obligations.

### 3. REVISE YOUR PRIVACY POLICY AND ENSURE OTHER REQUIRED PRIVACY NOTICES ARE PROVIDED

**EXPLANATION:** The CCPA and the regulations include specific disclosure requirements for businesses to include in their privacy policies. For example, consumer-facing privacy policies must disclose the categories of personal information collected, the sources of that information, how that information is used, shared, and sold, and an explanation of consumer rights under the CCPA. In addition to privacy policies, the regulations introduce requirements to present additional privacy notices, such as notices at collection, notices of sale opt-outs, and notices of financial incentives. All of these privacy notices are required to be in a format that meets accessibility requirements and, under certain circumstances, translated into other languages. Finally, the CCPA requires businesses to refresh their privacy policies at least every 12 months. As you update your policy for CCPA now, develop a plan to revise your policy on an annual basis as well.

Businesses should also revise their employee privacy policies to ensure that employees are informed, at or before the point of collection, of the categories of personal information that will be collected from them and the purposes for which these categories of personal information will be used.

**CCPA STARTER KIT RESOURCES**

- Privacy Policy Checklist
- Accessibility Guidelines
- Financial Incentives Guidance

**OTHER WAYS PERKINS COIE CAN HELP**

We write and review hundreds of privacy policies each year and can help benchmark your disclosures against industry practices and legal developments as they emerge. Some companies choose to have Perkins Coie draft their updates, whereas others draft the updates themselves and have Perkins Coie review all their changes.

### 4. DEVELOP A PLAN FOR RESPONDING TO CONSUMER RIGHTS REQUESTS

**EXPLANATION:** The CCPA articulates several rights consumers have with respect to their personal information. Specifically, the CCPA grants consumers the following:

- **Right to Know:** Request additional transparency about a company's information practices, including the categories of personal information you collect and share, among other details.
- **Right to Access:** Request specific pieces of personal information, sometimes in a portable format.
- **Right to Deletion:** Request deletion of a consumer's personal information (subject to broad exceptions).
- **Right to Stop Sale:** Opt-out of sale (opt-in for children 16 and under (by parents for those under 13)).
- **Right to Non-Discrimination:** Consumers that exercise their privacy rights have a right to equal service and price from the business, although some financial incentives are permitted.

Your company will need to develop and implement a process for receiving, confirming receipt, authenticating, reviewing, and responding to requests from consumers within the statutory timeframe (typically 45 days). It will also need to maintain records of consumer requests and associated responses for at least 24 months under the regulations. These CCPA

compliance requirements involve significant coordination with your technology and operations teams. Some companies extend CCPA rights to all of their users, whereas others restrict to CA residents. To identify the information that you will need to delete or disclose in response to consumer requests, you should analyze when exceptions articulated under the CCPA apply to information collected or retained by your company. Finally, you will need to determine the two or more methods you will provide for consumers to submit rights requests (such as an email address, toll-free phone number, or interactive webform, depending upon how your business operates).

**CCPA STARTER KIT RESOURCES**

- Consumer Rights Playbook, which includes the following customizable elements:
  - Internal policy explaining your company's principles and processes for receiving, reviewing, and responding to consumer rights requests
  - Step-by-step checklists for each type of request
  - Template responses for each type of request
- Interactive Webform Template
- Template Request Tracking Log
- Exceptions Analysis
- Data Map Template

**OTHER WAYS PERKINS COIE CAN HELP**

Some clients engage us to assist with completing the Exceptions Analysis template included in the Starter Kit to analyze how and when statutory exceptions could limit the scope of their obligations to comply with consumer rights requests under the CCPA. We can also work with you to customize the Consumer Rights Requests Playbook, or we can review your proposed customizations to that document.

## 5. REVIEW AGREEMENTS WITH VENDORS AND THIRD PARTIES

**EXPLANATION:** As noted in #2 above, the CCPA exempts disclosures to "service providers" from the types of data sharing that constitutes "sales" under the statute. As part of your data mapping effort, your company will identify vendors and other partners with whom you share information, such as email marketing providers, web hosting services, etc. Review these agreements to ensure they satisfy the definition of "service provider," do not trigger CCPA "sales" obligations, and prohibit the vendor from using the personal information your company shares for any purpose other than to perform the services.

Consider implementing data processing addenda with high-risk vendors; the CCPA Starter Kit contains a template data processing addendum. Other vendor agreements could be updated for CCPA purposes during the normal renewal cycle, provided that your company is comfortable taking a more risk-based approach. If you do not already have one, establish a process for vetting new service providers as well as policies and procedures for auditing service providers' compliance with their respective privacy and security obligations.

**CCPA STARTER KIT RESOURCES**

- Guidelines for Service Provider Agreements
- Template Data Processing Addendum
- Sales Analysis
- Privacy by Design Checklist

**OTHER WAYS PERKINS COIE CAN HELP**

Some clients to engage us to review, revise, and negotiate some or all of their service provider agreements.

## 6. TRAIN EMPLOYEES

**EXPLANATION:** The CCPA requires that personnel who will participate in your company's processes for accepting, reviewing, and responding to consumer rights receive appropriate training. Start by identifying who within your company will play a role in handling consumer rights requests. Provide general awareness training to all employees and contractors and specialist training to the individuals who will be on the front lines of receiving and responding to consumer requests. Keep records of trainings and consider requiring a proficiency assessment, particularly for individuals who will handle consumer requests directly.

**CCPA STARTER KIT RESOURCES**

- Employee Training Materials

**OTHER WAYS PERKINS COIE CAN HELP**

Some clients prefer Perkins to conduct training on-site or via video conference with their employees. We also offer legal office hours to help answer questions from your various operational teams that will be participating in your CCPA compliance effort.

## 7. CONDUCT A SECURITY CHECK-UP

**EXPLANATION:** The CCPA includes a limited private right of action for data breaches reportable under existing law (e.g. breach of data such as name + account number, SSN, or similar sensitive data) that occur because of a business's failure to implement reasonable security measures. A security review will help you ensure your company has proper protections in place to mitigate risks related to data breaches (and the attendant private right of action). Work with your IT/InfoSec teams to review existing data security measures and ensure a level of security appropriate to the risk posed by the personal information you collect or receive and whether new or additional data security measures should be implemented (e.g., pseudonymization, encryption, and/or access controls). Review your practices against data security guidance issued by the California Attorney General in 2016. Preparing for CCPA compliance also offers a good opportunity to review and update your incident response plan to comply with applicable law.

**CCPA STARTER KIT RESOURCES**

- Template Data Security Policy

**OTHER WAYS PERKINS COIE CAN HELP**

Perkins works with companies on all aspects of building their data security programs. We offer a tracker of all state data breach notice laws (available here). If you do not yet have an incident response plan in place, Perkins Coie's data security attorneys can work with you to customize our template. Perkins Coie attorneys also have experience conducting table-top exercises to evaluate and improve breach preparedness.

## 8. ATTEND TO ONGOING PRIVACY GOVERNANCE

**EXPLANATION:** Develop a plan for reviewing and vetting new products, services, or data-sharing plans to ensure privacy and data security are appropriately considered. Some companies refer to this as "Privacy by Design." You should also consider creating a privacy governance committee or other reporting/stakeholder engagement structure that fits your business. Schedule regular reviews and updates to your data map and governance documents to ensure they remain relevant and current. Even if applicable laws remain the same, changes to industry norms and best practices may merit updates.

**CCPA STARTER KIT RESOURCES**

- Privacy by Design Checklist

**OTHER WAYS PERKINS COIE CAN HELP**

Perkins Coie can help customize documents and processes to aid your company's ongoing privacy compliance. Some companies prefer robust internal policies, whereas other companies opt for checklists and trainings to help communicate privacy principles and expectations across the organization.