7 Steps to Comply with the CCPA

Insights
5.24.23

Getting into compliance with the California Consumer Privacy Act (CCPA) can seem like an overwhelming task. After all, the law is comprised not only of a dense statute and detailed regulations, but the amendment effective January 1, 2023 has added to the complexity by removing the exemptions for data collected in the employment and B-2-B contexts. But there's good news. Businesses subject to the law can take the below seven steps to achieve full compliance.

A word of caution, however. These compliance steps can take six to twelve months to complete, and are best handled by working closely with data privacy counsel. With the help of Fisher Phillips' Consumer Privacy Team, your preparations can be fast-tracked. Our knowledgeable team has prepared a menu of flat-fee starter kits, templates, packets, and other resources to jumpstart the process. Please reach out to your Fisher Phillips contact to learn more about all of our CCPA/CPRA services.

1. Inventory and map all consumer data, including employee and job applicant data.

Understand pertinent defined terms such as what is "personal information" and "sensitive personal information," who is a California "consumer" (including employees and job applicants), and what constitutes "collection" under the regulations to frame the scope of any data inventory or mapping exercise.

- Consider the various sources, channels, or points at which you collect data from a consumer, and at what date and time the collection occurs.
- Evaluate the business purpose for which you collect and process any information, and with whom it is shared. Are there any service providers or third parties (as these entities are defined in the regulations) who store or process any consumer data on your behalf?
- Identify the location in which data is stored and who has access to the data, and determine applicable retention periods for each category of personal and sensitive personal information collected.

2. Take appropriate steps to secure all consumer and employment-related data.

In support of the obligation to secure consumer data, you may be required to conduct an annual security assessment depending on risk factors and sensitivity of the data you collect or maintain.

- The implementation of reasonable security procedures and practices may include a review of any cyber and/or information security policy(ies) and incident response plans.
- Any security review should evaluate the security measures of service providers, contractors and third parties and include updating agreements to comply with CCPA requirements.

3. Prepare and provide a "notice at collection" to all consumers (including employees and job applicants) at or before collecting any consumer data.

Review the content requirements for the Notice at Collection and update for compliance with the CCPA regulations effective March 29, 2023.

- Evaluate where data is collected (for example online, in-person, or telephonically) and ensure the Notice at Collection is available at such location.
- Make sure you distribute the notice to job applicants as well as new and current employees.

4. Prepare and post a comprehensive privacy policy on your website.

- Make sure it includes more than just the Notice at Collection, providing employees with a privacy policy pertaining to all employment-related data explaining how they can exercise their CCPA rights.
- Ensure the privacy policy includes all required content under by the CCPA, including, but not limited to, whether any data is sold (which includes any sharing of data with a third party that is not a "service provider" in exchange for valuable consideration).

5. Deploy a process to receive and respond to consumer requests from all consumers (a process referred to by many privacy practitioners as DSR or data subject request, although the term is not used in the CCPA).

Implement a consumer request process that can address all the types of requests a consumer can make under the CCPA, including, but not limited to, the right to know, request to delete, request to correct and the request to opt out of the sale of personal information. Since January 1, 2023, consumers can submit a request to correct information and request to limit the use or disclosure of sensitive personal information.

- You must implement at least two methods for CCPA requests and adhere to strict response deadlines.
- In addition, you must implement a verification process to verify the identity of the person making a request.

6. Implement data minimization rules.

This includes a data retention policy and workflow for purging stale data for which there is no legal or business reason to keep.

7. Train all managers and employees on all CCPA requirements in which they play any role.

This may include those responsible for CCPA compliance and anyone directly interacting with consumers and providing information, notices, and forms, or assisting with the business's response to any CCPA request.

Conclusion

Compliance with consumer privacy laws is not a matter of distributing templates that are turnkey or "plug and play." Rather, compliance is an ongoing and individualized process, and all the requisite forms, templates, notices, and policies must be tailored for your business.

Whether you have already completed the first round of CCPA compliance but need guidance on the CPRA amendments, or you are unsure of whether the requirements apply to your business and don't know where to begin, or you are somewhere in between, Fisher Phillips is here to help. Our Consumer Privacy Team's menu of compliance packages and services is designed to fit any business, no matter what your needs are.

Fisher Phillips will continue to monitor CCPA obligations and enforcement efforts and provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insights to get the most up-to-date information direct to your inbox. For further information, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on the firm's Consumer Privacy Team.

Related People

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Darcey M. Groden, CIPP/US
Associate
858.597.9627
Email

Anne Yarovoy Khan
Of Counsel
949.798.2162
Email

Jenna Rogenski
Associate
415.490.9013
Email

Christopher M. Champine
Associate
858.597.0278
Email

Anthony Isola
Partner
415.490.9018
Email

Benjamin M. Ebbink
Partner
916.210.0400
Email

Service Focus

Data Security and Workplace Privacy

Consumer Privacy Team

Emerging Issue Focus

CCPA Resource Center

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills