

CCPA Update: Preparing for the CCPA – 10 Things You Can Tackle Now

The Bottom Line

- *In the ever-changing landscape of the U.S. privacy space, businesses should not take a wait-and-see approach when it comes to CCPA compliance.*
- *The ten action items outlined in this Alert will not only assist businesses with CCPA compliance, but may also assist with compliance with other new privacy laws and standards and serve as best practices.*

While the California Consumer Privacy Act (CCPA) promises to bring significant change to the way some businesses collect and use personal information from consumers, the exact scope of that change remains unclear. Businesses must wait for the California Attorney General to issue implementing regulations in order to gain greater clarity on how key CCPA provisions will be enforced and interpreted, while at the same time some amendments have been enacted and further amendments proposed, including within the past week.

Actual enforcement of the CCPA will not begin until the earlier of six months after such regulations are issued or July 1, 2020. However, the law is still set to become effective January 1, 2020 and businesses should not wait on the Attorney General before taking action. Compliance with the CCPA will require far more than just surface-level cosmetic changes to a website's privacy policy. For example, businesses will need to maintain records of their data processing activities and be able to respond to consumer data access requests.

As was the case with the rollout of the European General Data Protection Regulation (GDPR), and since compliance will take time to achieve, certain preparations should be taken now – well in advance of any potential enforcement — to meet the CCPA's many obligations, including updating internal processes and procedures.

1) Assess the CCPA's applicability to your business

Determine whether your business falls within the scope of the CCPA. The CCPA applies to businesses that collect California consumers' personal information and either (i) have annual gross revenues in excess of \$25 million, (ii) process the personal information of 50,000 or more California consumers, households, or devices or (iii) derive 50 percent or more of their annual revenues from selling California consumers' personal information. Note that the CCPA has broad applicability and protects the information of California residents (not only when they are present in California). This means that certain "geo-fencing" strategies that were used to avoid the applicability of the GDPR may not be sufficient in the case of the CCPA.

2) Review and track your data collection practices and data streams

It's important to have a firm understanding of what personal information your business is collecting, how the personal information is being processed, and with whom the personal information is being shared. The CCPA will require you to disclose collected data to consumers who request it and to inform consumers of

your data collection practices before you collect personal information. If your business has not already done so, consider creating system diagrams that document the lifecycle of collected data and data flow maps for locating a customer's personal information. This will also help with your recordkeeping efforts.

3) Maintain records of data processing activities

Under the CCPA, a California consumer is entitled to request that a business provide certain disclosures as they relate to the processing of that consumer's personal information within the year preceding the request in a readily usable format. This is sometimes referred to as the "look back" provision. Since consumers can start exercising their rights and requesting information about a business's data processing activities on January 1, 2020, this technically means that a year prior to such possible request, businesses should be keeping records on their processing activities in a way that enables them to respond effectively to this "look back" provision. The recent amendments to the CCPA did not postpone the applicability of the "look back" provision. Because the Attorney General's approach to enforcement is unclear at this time, businesses will need to have processes in place to organize and manage consumer data collected well before the Attorney General commences enforcement activities.

4) Review policies and identify gaps with GDPR

There is a common misconception that being GDPR compliant means you are also CCPA compliant. This is not the case. Businesses should certainly coordinate their GDPR and CCPA compliance efforts, but also be mindful of the differences. For example, the CCPA explicitly restricts discrimination against consumers that have exercised their rights under the CCPA, including by charging different prices for services or providing a different level of services. Businesses should take steps to uncover gaps in their current practices that are not yet CCPA-compliant, identify operational challenges that CCPA compliance may pose and plan for compliance action.

5) Review external privacy policies and other consumer disclosures

The CCPA requires certain disclosures to be made to consumers. Reviewing existing disclosures and commitments currently made by the business can help identify any missing disclosures and commitments required under the CCPA.

6) Plan how to proactively communicate with your consumers about CCPA compliance

Devise a uniform public-facing message that communicates to your consumers and clients about the business's position on CCPA compliance. This message can be used whenever a consumer or a corporate client asks about CCPA. The message should be disseminated within the business to ensure that employees understand how to effectively communicate the business's position on CCPA.

7) Stay up-to-date on state and federal privacy developments

The CCPA will not be the last data privacy regulation your business will have to address. There are numerous new state laws pending, including proposed laws in Washington State and New York. The Federal Government has also introduced various new privacy bills, including one that can preempt state law, including the CCPA. Staying current on privacy developments and frequently conversing with your privacy counsel will help you prepare for and react more appropriately to legal changes that impact your business.

8) Assess third parties

One of the major requirements under the CCPA is to provide consumers with the opportunity to opt-out of the “sale” of their personal information. The standard is opt-in if the user is under 16 years of age. The definitions of “personal information” and “sale” are both extremely broad. Further, a business is provided with a safe harbor for non-compliance by their service providers if certain controls with the service provider have been put in place. Therefore, consider all third parties with whom the business is working and the contracts with such third parties, both in terms of parties to whom data is transferred and counter-parties when the business is a recipient of data.

9) Be flexible

While it is best to take action even while the industry waits for regulations from the Attorney General, every organization will need to be flexible should the regulations move the goal posts on your plans. The CCPA was amended in September 2018 (please see our alert titled, “California Legislature Passes Yet More Privacy Bills – Internet of Things & CCPA Amendment”) and another amendment was proposed in February 2019 which would significantly expand the private right of action and also eliminate a cure period under the law, thus greatly increasing the potential exposure to companies. (For additional information on the CCPA, please see our alert titled, “CCPA Update: California Public Forums and Other Proposed State/Federal Legislation.”)

10) Consult with your privacy counsel

Work with outside legal counsel that is well-versed in privacy law and the CCPA in particular. Due to the complexities and current uncertainties of the CCPA, the legal, regulatory and technical implications of the CCPA and other privacy laws could have a significant impact on your business’s data processing activities.

Related People

Richard S. Eisert

Partner/Co-Chair Advertising + Marketing

212 468 4863

reisert@dglaw.com

Gary Kibel

Partner

212 468 4918

gkibel@dglaw.com