90 Days Until CPRA Enforcement: A Compliance Roadmap

Lizzi Esparza
eesparza@mwlaw.com
(479) 464.5660

10/03/2022

All businesses – not just those located in California – should be aware of changes to California's data privacy law. In 2018, California passed the California Consumer Privacy Act ("CCPA"), a first-of-its-kind consumer privacy law granting consumers certain rights in their personal information. Two years later, Californians passed the California Privacy Rights Act ("CPRA") that added protections for consumers and obligations for businesses. The CPRA is set to go into effect on January 1, 2023. The Attorney General of California has signaled an intention to strongly enforce this law,[1] making it important to ensure that your business is compliant from the start.

STEP ONE: Are you subject to the new law?

The CPRA expanded definitions and obligations of different types of entities. If you were subject to the CCPA, chances are high that you will also be subject to the CPRA, but it is important to understand how you are classified under the new law, and the new obligations that follow.

Businesses

The CPRA has expanded the definition of a business to include any for-profit entity doing business in California (whether or not that business is resident to California) that collects California consumers' personal information and (1) had annual gross revenues of more than $25 million in the previous year, (2) buys, sells, or shares personal information of 100,000 California consumers or households, or (3) derives 50% or more of its annual revenue from selling or sharing information.[2]

Ambiguity surrounding the word "sell" has been removed by instead including businesses who "share" data. Here, "share" encompasses activities such as "sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating" personal information, but notably, the information must be shared with a third party for cross-context behavioral advertising to be considered shared.[3] In other words, if your business discloses California consumer information to a third party for the purposes of delivering targeted ads, you may now be a "business" subject to the requirements of CPRA even though you are not "selling" the information.

Service Providers, Contractors, and Third Parties

Service Providers include anyone who processes California consumer personal information on behalf of a business pursuant to a written contract. Slightly distinguished, a Contractor is a person to whom a business makes California personal information available pursuant to a written contract. If you or your business does not fall into either of these categories, you may still be subject to the provisions of this law as a Third Party if you receive California consumers' personal information from a covered business.[4]

The CPRA requires certain contractual provisions be included in the agreements between Businesses and Service Providers or Businesses and Contractors, including a prohibition on the sale or share of personal information, a requirement to notify the business of sub-processors, and a provision regarding monitoring of compliance. Businesses should check their existing service agreements to ensure that they meet these new requirements, and revise as necessary.

STEP TWO: Update your Privacy Policy and Notices to California Consumers.

In addition to the categories of data collected and the purposes for use, businesses must now notify their California consumers of the purposes for which the information is collected or used, whether the information is sold or shared, and the length of time the business intends to retain the information, and the consumer's right to opt out. This notice needs to be provided "at or before the point of collection."[5]

The CPRA also requires businesses to identify in a Privacy Policy the categories of third parties to whom information is disclosed or sold, the business or commercial purpose for collecting or selling personal information, and the categories of sources from which personal information is collected. In addition to certain form and language updates, your Privacy Policy will need to be updated to reflect the additional rights that the CPRA granted to consumers, such as the right to correct inaccurate personal information, and the right to limit use and disclosure of sensitive personal information.[6]

Whether starting from scratch or just updating an existing CCPA Privacy Policy, it is important that a business take the time to ensure compliance with these new requirements.

STEP THREE: Prepare or update internal policies and processes.

Your business should be prepared to respond to consumers who choose to exercise their new rights under the law. For example, under the CPRA, consumers now have the right to request that a business limit the use of their sensitive personal information, which refers to specific types of data (when it is publicly unavailable), including precise geolocation, contents of email and text messages, and information concerning a consumer's health.[7] It will be important to not only ensure that your business complies with the CPRA's requirements of notifying California consumers of this right, but also actually have a plan in place to be able to limit the use of that data.

In addition to the new rights provided to California consumers, businesses have new obligations under the law. For example, a business may not retain a California consumer's personal information for longer than is reasonably necessary and may only gather the scope of data proportionate to the purposes it was collected or processed for.[8] Creating a data retention policy – or updating an existing one – that specifies the purpose for which the data was collected, and then enforcing same through your data collection, processing, and retention, can help your business comply with this provision.

Finally, California consumers may request the specific pieces of personal information that a business has about them. If a business cannot or has not deidentified or aggregated this information, it will need to provide that information to the consumer in a commonly used, machine-readable format. If a customer requests the information be deleted, the business must permanently delete the information within 45 days. Creating a policy to ensure that data is properly mapped and stored can help facilitate your ability to timely respond to these requests.

Future Developments

Businesses should keep an eye out for future state regulations pertaining to obtaining consent from their California consumers, the use of automated decision-making technology, and requirements for cybersecurity audits. As the deadline for compliance rapidly approaches, businesses need to be mindful of their newfound obligations for data they hold about California residents, even when they are located far from California.

[1] Office of the Attorney General of California, *Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act*, August 24, 2022, https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement.

[2] Cal. Civ. Code § 1798.140(d).

[3] § 1798.140(ah)(1).

[4] § 1798.100(d)(2)-(4).

[5] § 1798.100.

[6] § 1798.130(a)(5).

[7] § 1798.121.

[8] § 1798.100(a)(3).