Client Alert: Updated Regulations Under the California Consumer Privacy Act (CCPA)

By:Kevin S. Olson and Faith D. Kasparian
December 15, 2025

The California Privacy Protection Agency (the CPPA, which recently rebranded as CalPrivacy) has finalized regulations addressing several areas, including: automated decisionmaking technology (ADMT, which is the term used to refer to AI), risk assessments, and cybersecurity audits, as well as several other important aspects of the existing CCPA regulations. There are several staged compliance deadlines for each of these areas, with many provisions scheduled to take effect on January 1, 2026, and others taking effect in the years between 2026-2030.

1. Automated Decisionmaking Technology (ADMT)

The new ADMT regulations address the use of artificial intelligence programs to make "significant decisions" about individuals. Similar to other AI laws such as the EU AI Act or the Colorado AI Act, significant decisions are limited to certain high-risk areas, such as a decision that results in providing or denying financial or lending services, housing, education enrollment, employment, or healthcare services. And, at a high level, in relevant part, the regulations apply when these decisions are made with ADMT that replaces or substantially replaces human decisionmaking.

If a business is using ADMT to make significant decisions, among other obligations, they must provide individuals with pre-use notice detailing the specific ADMT uses and their rights, including the right to opt out of such use of ADMT and the right to access information on how decisions are made. And, it is only possible to take such use of ADMT outside the scope of these regulations if there is a sufficient level of human involvement, namely where a human reviewer knows how to interpret and use an output to make the decision; can review and analyze the output, and any other information that is relevant to make or change the decision; and has the authority to make or change the decision based on their analysis.

The obligations with respect to ADMT are effective January 1, 2027.

2. Risk Assessments

Similar to many other U.S. state privacy laws that have a requirement to conduct a data protection impact assessment (DPIA) for certain activities, the new regulations introduce a risk assessment requirement for processing activities that present a significant risk to an individual's privacy. Examples of such high-risk activities include selling or sharing personal information, processing sensitive personal information, and using ADMT for significant decisions.

The risk assessment process requires businesses to document and weigh whether the risks to individual privacy outweigh the benefits to consumers, the business, stakeholders, and the public. Among other criteria, the assessment must include specific information on the purpose and scope of processing, the categories of personal information processed, and planned safeguards such as encryption or privacy-enhancing technologies.

These regulations go into effect on January 1, 2026, and businesses must submit the risk

assessment to CalPrivacy. For risk assessments completed in 2026 or 2027, the risk assessment must be submitted to CalPrivacy in 2028; for risk assessments completed after 2027, the risk assessment must be submitted to CalPrivacy no later than April 1 following any year during which the business conducted the risk assessments.

3. Cybersecurity Audits

The regulations also mandate an annual cybersecurity audit for businesses whose processing presents significant security risks to consumer data. Processing constitutes a significant risk where:

- (i) a business derives 50% or more of its revenue from the selling or sharing of personal information; or
- (ii) for businesses meeting the CCPA's revenue threshold, where the business
  - (a) processed the personal information of 250,000 or more California residents or households in the preceding calendar year; or
  - (b) processed the sensitive personal information of 50,000 or more California residents in the preceding calendar year.

However, these audit requirements will be phased in based on annual gross revenue as detailed in the table below:

Annual Gross Revenue	Due Date	Period Covered
Over $100 million (as of Jan. 1, 2027)	April 1, 2028	Jan. 1, 2027–Jan. 1, 2028
$50 million–$100 million (as of Jan 1, 2028)	April 1, 2029	Jan. 1, 2028–Jan. 1, 2029
Less than $50 million (as of Jan 1, 2029)	April 1, 2030	Jan. 1, 2029–Jan. 1, 2030

After April 1, 2030, any business that meets the audit criteria for the previous year must complete a cybersecurity audit and submit the report by April 1 of the next year.

These audits must evaluate several specific components of cybersecurity programs, including encryption, incident response, and oversight of service providers. In particular, for each calendar year that a business is required to complete a cybersecurity audit, the business must submit a written certification to the CalPrivacy that the business completed the required cybersecurity audit.

4. Changes to Requirements Regarding Opt-Out Preference Signals (OOPS)

In addition to the above areas, CalPrivacy also revised several sections of the existing regulations that address the processing of OOPS. Under the previous regulations, businesses were given the option to: (i) display that an OOPS has been processed; and (ii) allow an individual to confirm their opt-out status. Under the revised regulations, businesses are now required to display whether the OOPS has been processed, such as by displaying the text "Opt-Out Request Honored" and using a toggle or radio button to indicate the consumer has opted out of the sale/sharing of their personal information. In addition, the business must also provide a means for a consumer to confirm their opt-out status.

Given that these particular provisions are effective on January 1, 2026, businesses that engage in the sale and/or sharing of personal information should reassess their processing of OOPS. It is

also worth noting that CalPrivacy had recently announced an investigative sweep with the Colorado and Connecticut attorneys general regarding compliance with OOPS.

Looking Ahead

Businesses should carefully consider what AI products they are using as well as anticipated use cases, determine whether they need to conduct a risk assessment, review their audit processes, review their privacy notices to ensure they remain accurate, and reassess their current opt-out mechanisms.

If you have any questions about these revised CCPA regulations, or if you have any other data privacy or security related questions, please reach out to Kevin Olson, Faith Kasparian, Ryan Perry, or Ann O'Rourke.

This Alert provides general information only. It is not intended to provide advice with respect to any specific set of facts, nor is it intended to advise on all developments in the law.