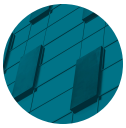
WILSON SONSINI

CPPA Approves New CCPA Regulations on AI, Cybersecurity, and Risk Governance, and Advances Updated Data Broker Regulations

CONTRIBUTORS


Tracy Shapiro


Eddie Holman


Angela Guo

ALERTS

July 30, 2025

On July 24, 2025, the California Privacy Protection Agency (CPPA) Board voted to approve a long-awaited rulemaking package imposing substantial new compliance obligations on businesses subject to the California Consumer Privacy Act (CCPA). The package contains finalized rules on AI-related, automated decision-making technologies (ADMT), cybersecurity audits, and risk assessments, as well as updates to existing CCPA regulations. These regulations will impact a broad swath of businesses handling personal information of California residents.

The CPPA Board's approval of the new regulations is the culmination of a year-long process that began when the agency first released draft regulations on these topics in July 2024 and initiated the formal rulemaking in November 2024 (analyzed in prior Wilson Sonsini client alerts). In April and May 2025, the Board grappled with public concerns from hundreds of public comments on the draft regulations, analyses of which can be found in these recent client alerts.

In addition, the CPPA Board approved modifications to the proposed data broker regulations concerning the Delete Request and Opt-Out Platform (DROP) mandated by the Delete Act (discussed in a prior post). These modifications will be subject to a new 15-day public comment period once the agency publishes official notice of the changes.

Below is a summary of the new regulations, timelines for compliance, and other updates from the July 24, 2025, Board meeting.

New CCPA Regulations

In a 5-0 vote, the CPPA Board voted to adopt the draft regulations regarding ADMT, risk assessments, cybersecurity audits, insurance, and updates to existing regulations. The substance of the new regulations have not changed since the previous draft was released and discussed at the May Board meeting, discussed in a prior client alert.

Below is a high-level summary of the new regulations, including timing and operational implications for businesses preparing for implementation.

Automated Decision-Making Technology (ADMT)

The new regulations require businesses that use ADMT to make a "significant decision" concerning a consumer to fulfill certain notice, opt-out, and access request obligations.

- *ADMT Defined*: The new regulations define ADMT to mean any technology that processes personal information and uses computation to *replace or substantially replace* human decision

making. "Substantially replace" means a business uses the ADMT's output to make a decision without human involvement.

- *Significant Decisions*: The new regulations define "significant decision" to mean a decision that results in the provision or denial of financial or lending services, housing, education enrollment or opportunities, employment or independent contracting opportunities or compensation, or healthcare services. Advertising to a consumer is specifically excluded from the definition.
- *ADMT Obligations*: Businesses that use ADMT to make a "significant decision" concerning a consumer are required to:
  - provide pre-use notices to inform consumers about the business's use of ADMT and the consumer's rights to opt out and access further information;
  - allow consumers to opt out, with limited exceptions; and
  - grant consumers access to information about the ADMT's use and logic.
- *Timeline*: The ADMT regulations come into effect on the effective date of the regulations, which is not yet determined. See additional details on when the regulations will take effect under "Next Steps," below.

Cybersecurity Audits

The new regulations will require annual independent cybersecurity audits for businesses whose processing activities pose "significant risk" to consumers' security, as broadly defined in the new regulations.

- *Applicability*: A business engages in processing activities that pose a "significant risk" to consumers' security and hence must undergo an audit if, in the last calendar year, it 1) meets the CCPA revenue threshold to qualify as a "business" (currently $26.625 million) *and*, in the preceding calendar year, processes the personal information of 250,000 or more consumers or households *or* processes the sensitive personal information of 50,000 or more consumers; or 2) derives at least 50 percent of its annual revenues from selling or sharing California residents' personal information.
- *Audit Scope and Requirements*: Audits must assess every applicable component of the business's cybersecurity program, including 18 specifically identified components that include authentication, encryption, access controls, inventory management, scans, logging, technical configurations, training, software development, incident response, disaster recovery, and third-party oversight, among others. Businesses must document identified gaps, mitigation efforts, and copies of breach notifications issued during the audit period. Audit findings cannot rely primarily on assertions or attestations by management. Rather, they must be evidence-based and supported by documents, sampling, testing, and interviews. All audit related documents must be kept for five years.
- *Certification to CPPA*: A member of the business's executive management team who is directly responsible for audit compliance, has sufficient knowledge of the audit to provide accurate information, and has the authority to submit the business's certification to the agency must certify that the business completed the cybersecurity audit and attest that the business did not attempt to influence the auditor's decisions or assessments. The business does not need to provide the underlying audit results as part of the annual certification.
- *Auditor Requirements*: Cybersecurity audits must be conducted by a qualified, objective, independent auditor using generally accepted procedures and standards and having knowledge of cybersecurity and how to audit cybersecurity programs. If businesses use internal auditors, the new regulations impose additional obligations governing the auditor's reporting chain and performance reviews to preserve their independence.
- *Phased Timeline*: The requirement to conduct cybersecurity audits will be rolled out on a phased schedule according to a business's annual gross revenues. Businesses with annual gross revenue above $100 million in 2026 will be subject to the first deadline and must complete audits for 2027 by April 1, 2028. Smaller businesses are subject to similar requirements over the course of the following two years. All businesses meeting the general audit applicability requirements will have to complete audits for 2029 by April 1, 2030.

Risk Assessments

Businesses must conduct a detailed risk assessment before initiating certain activities that present "significant risk" to consumers' privacy and submit risk assessment summary information and attestations annually to the CPPA.

- *Applicability*: Activities that present a "significant risk" include: 1) selling or "sharing" personal information, 2) processing sensitive personal information, 3) using ADMT for significant decisions, 4) using automated processing to infer a consumer's intelligence, ability, aptitude, work

performance, economic situation, health, personal preferences, interests, reliability, predispositions, behavior, location, or movements based on the consumer's presence in a sensitive location *or* observations of the consumer in their capacity as an applicant, student, employee, or independent contractor, and 5) processing personal information to train ADMT systems to make significant decisions or to train biometric ID verification and profiling systems.

- *Risk Assessment Requirements*: At a high level, risk assessments must include:
  - the purpose of the processing;
  - categories of personal information to be processed;
  - operational elements of the processing, including the methods for processing personal information and interacting with consumers, how long personal information will be retained, the number of consumers whose personal information will be processed, what disclosures will be made to consumers and how, what other parties will be involved in the processing and for what purposes, and certain uses of ADMT;
  - expected benefits to the business, consumer, other stakeholders, and the public;
  - negative impacts to consumers' privacy and safeguards to address the impacts;
  - whether the business will initiate the processing; and
  - individuals involved in preparing, reviewing, and approving the risk assessment.

- *Submissions of Attestations to the CPPA*: Businesses must submit to the CPPA an attestation by an executive that the business has conducted a risk assessment that meets the regulation's requirements, information about the number of risk assessments conducted or updated for each of the processing purposes that can trigger a risk assessment, and whether the risk assessments involved the processing of each of the CCPA's personal information and sensitive personal information categories. Full risk assessment reports must be available for inspection upon request by the CPPA or Attorney General.
- *Timing of Risk Assessments*: For preexisting covered activities (i.e., covered activities that businesses initiated before the new regulations' effective date and engaged in after the effective date), businesses must conduct risk assessments by December 31, 2027, and submit attestations to the CPPA by April 1, 2028. For covered activities that businesses initiate in 2026 and 2027, businesses must conduct risk assessments before engaging in those activities and submit attestations by April 1, 2028. For covered activities that businesses initiate after 2027, businesses must submit attestations by April 1 of the following year. Businesses also must review all previously conducted risk assessments at least once every three years and update them as necessary to ensure they remain accurate, or within 45 days of any material change to the covered processing activity.

Key Changes to Existing Regulations

The new regulations also amend and clarify certain core CCPA compliance requirements. Notable updates include:

- requiring businesses to display a clear indication of whether they have honored a consumer's request to opt out of sale or sharing, for example by displaying "Opt-Out Request Preference Signal Honored" when a consumer using an opt-out preference signal visits the website and displaying the status of the consumer's choice in the consumer's privacy settings through a toggle or radio button;
- requiring notices of the right to opt out of sharing/sales and to limit the use of sensitive information in a manner that ensures consumers will encounter the notice before or at the time data collection begins on connected devices or in augmented or virtual reality environments (*or* before or at the time the consumer encounters the business in AR/VR environments); and
- clarifying requirements regarding "symmetry in choice" for methods of submitting CCPA requests and obtaining consumer consent, specifically that user interfaces must offer equal visual prominence for "yes" and "no" choices.

Some Public Comments Left Unresolved

Public comments from labor unions, consumer advocates, and civil society groups overwhelmingly expressed concern over perceived "weakening" of the new regulations, warning that narrowed definitions and reduced safeguards would leave workers, consumers, and small businesses vulnerable to the harms of algorithmic decision making while favoring corporate interests and undermining the CCPA's intent. One recurring concern was a lack of clarity in key definitions, particularly for the definition of ADMT, which commenters argued could effectively allow businesses to opt out of the rules by claiming their algorithmic tool is merely advisory. Small businesses, on the other hand, raised concerns about the operational burden and cost of compliance. Additionally, commenters warned that the new regulations' breadth may unintentionally discourage innovation.

Nonetheless, CPPA staff believed that no additional changes to the new regulations were necessary, and the Board generally agreed. CPPA staff agreed, however, to produce a guide explaining why the agency should not be worried about the concerns expressed in public comments. In addition, CPPA staff offered to publish additional guidelines to clarify what would constitute a "material change" that would trigger the requirement to update a risk assessment.

Proposed Amendments to Data Broker Registration Regulations

The Board also voted 5-0 to approve for public comment additional proposed modifications to data broker regulations concerning the Delete Request and Opt-Out Platform (DROP). As mandated by the Delete Act (discussed in prior alerts), the DROP will allow California residents to submit a single request to delete all personal information held by all data brokers operating in the state. Data brokers would be required to access the DROP for updates every 45 days and delete the personal information of any California resident that matches the data broker's records unless an exception set forth in the CCPA applies.

Below is a summary of the latest modifications to the proposed DROP regulations:

- *California Resident Verification*: The CPPA will be tasked with verifying that submitted delete requests originate from actual California residents before the request is submitted and passed on to data brokers. This measure aims to reduce the risk of falsified DROP requests and ensure that only verified California residents can support delete requests after residency verification.
- *Data Standardization Requirements*: Data standardization requirements have been modified to include more specific information about how data brokers must compare their databases with the data provided by the DROP system. This standardization aims to enhance compliance by ensuring brokers follow a consistent method for assessing personal information related to consumers who have submitted delete requests.
- *Consumer Matching Standards*: The matching standards for consumer data have been updated to require a 100 percent match when comparing multiple identifiers from the DROP deletion list. This change reflects the updated functionality of the DROP system and aims to minimize erroneous deletions by data brokers.

Next Steps

The final rulemaking package regarding ADMT, risk assessments, cybersecurity audits, insurance, and updates to existing regulations will now go to the California Office of Administrative Law (OAL). Once the CPPA staff submits the new regulations, the OAL will have 30 working days to evaluate whether the rulemaking package complies with the California Administrative Procedure Act. Generally, the effective date of a regulation approved by OAL and filed with the Secretary of State is the first of the quarter following the filing date.

The package allows the OAL to fill in the effective date of the regulations, with the effective date for risk assessment requirements taking place no later than December 31, 2027. In practice, businesses should anticipate ADMT requirements taking effect on the general effective date of the regulations, while cybersecurity audit and risk assessment requirements will apply two years later.

As for the data broker regulations, with the Board's approval of the latest proposed modifications, the DROP regulations will enter a 15-day public comment period after formal publication.

The Board is scheduled to meet again on September 26, 2025. At the next meeting, Deputy Director Michael Macko plans to present the CPPA's annual enforcement report and priorities.

Wilson Sonsini Goodrich & Rosati routinely helps companies navigate complex privacy and data security issues. For more information or advice concerning your CCPA compliance efforts, please contact Tracy Shapiro, Eddie Holman, Angela Guo, or any member of the firm's Data, Privacy, and Cybersecurity practice. For more information or advice concerning your compliance efforts related to ADMT or artificial intelligence, please contact Scott McKinney, Eddie Holman, Maneesha Mithal, or any member of the firm's Artificial Intelligence and Machine Learning practice.