wiley

ALERT

California Finalizes Pivotal CCPA Regulations on AI, Cyber Audits, and Risk Governance

October 9, 2025

Following several years of intensive rulemaking, the California Privacy Protection Agency (CPPA) has finalized new regulations under the California Consumer Privacy Act (CCPA) that govern three critical areas: (1) mandatory privacy risk assessments, (2) annual cybersecurity audits, and (3) the use of automated decision-making technology (ADMT).

Companies subject to the CCPA have a new set of highly prescriptive regulations to assess and comply with, requiring immediate preparation for staggered compliance deadlines beginning in early 2026.

1. **Privacy Risk Assessments**

The new rules establish requirements for conducting, documenting, and submitting information to the CPPA about privacy risk assessments for processing activities that present a "significant risk" to consumers' privacy.

Threshold: Businesses must conduct a privacy risk assessment before processing personal information in a manner that "presents significant risk to consumers' privacy," which is defined in the regulations as: (i) selling or sharing personal information; (ii) processing sensitive personal information; (iii) using ADMT for a significant decision concerning a consumer; (iv) using automated processing to infer or extrapolate specific personal traits including intelligence, ability, economic situation, and personal preferences – either based upon systematic observation when the consumer is acting in certain capacities (e.g., employee or job applicant) or based upon a consumer's presence in a sensitive location; or (v)

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Alissa Lynwood
Associate
202.719.4527
alynwood@wiley.law

Practice Areas

Artificial Intelligence (AI)
FTC and Consumer Protection
Privacy, Cyber & Data Governance
State Privacy Laws
Telecom, Media & Technology

processing personal information, which the business intends to use to train an ADMT for a significant decision concerning a consumer; or train a facial-recognition, emotion-recognition, or other technology that verifies a consumer's identity, or conducts physical or biological identification or profiling of a consumer.

Key Requirements**:** The new rules set forth detailed requirements for the assessment, including rules about stakeholder involvement in assessments, as well as prescriptive rules about the content of the assessments. For example, assessments must identify the purposes, benefits, reasonably foreseeable risks, and proposed safeguards associated with the processing, in addition to the operational details like collection, process, retention periods, and disclosures. There are additional assessment requirements for processing personal information to train ADMT. The new rules state that the goal of the risk assessment is to restrict or prohibit processing if the risk to the consumer's privacy outweighs the benefits to the consumer, the business, other stakeholders, and the public from that same processing.

In addition to conducting the assessment, the new regulations establish requirements that the final document must be certified by a senior executive and retained for a minimum of five years or for as long as the processing continues. Businesses are also required to submit to the CPPA certain summary information about the assessment, as well as an attestation of compliance.

Compliance Timeline: Businesses must begin conducting these privacy risk assessments by January 1, 2026. Assessments must be completed before the relevant processing, and they must be reviewed and updated as necessary at least every three years, except for when there is a material change relating to the processing, in which case the assessment must be updated within at least 45 calendar days.

Regarding submission requirements, the first mandatory filing – which includes an attestation that the required privacy risk assessments were completed and a summary of the assessment information – is due to the CPPA by April 1, 2028, covering assessments conducted during 2026 and 2027. For privacy risk assessments conducted after 2027, the summary and attestation are due by April 1 of the following year.

2. **Cybersecurity Audits**

The new rules also establish mandatory annual cybersecurity audits for a defined group of businesses that meet cumulative thresholds related to revenue and data volume.

Threshold: The audit requirement applies when a business meets at least one of the following two thresholds:

(1) In the preceding calendar year, the business met the CCPA's annual gross revenue threshold (currently set at approximately $26.62 million) *and* either (a) processed the personal information of at least 250,000 consumers or households, *or* (b) processed the sensitive personal information of 50,000 or more consumers, *or*

(2) The business derives at least 50% of annual revenue from selling or sharing personal information.

Key Requirements: The new rules establish detailed requirements for conducting cybersecurity audits—both in terms of who can conduct the audit and the substance of what is audited, preparing an audit report, certifying completion of the audit, and recordkeeping.

- *Conducting the audit.* Audits must be conducted using an internal or external "qualified, objective, independent professional . . . using procedures and standards accepted in the profession of auditing," who meets certain standards laid out in the rules. Overall, the audit is intended to assess the business's cybersecurity program, including how the business protects personal information from unauthorized access, destruction, use, modification, or disclosure, as well as how it protects against unauthorized activity resulting in the loss of availability of personal information. The rules outline 18 specific components of a cyber program that must be assessed, covering areas including authentication, encryption, incident response, service provider oversight, and network segmentation.
- *Preparing the audit report.* The rules also outline what must be included in the audit report, including a report on gaps or weaknesses in the program and the business's plan to address them. Ultimately, the audit report must be provided to a member of the business's executive management team who has direct responsibility for the business's cybersecurity program.
- *Certifying completion.* A written certificate of completion, signed by a member of the executive management team who has direct responsibility for the business's cybersecurity audit compliance and sufficient knowledge and authority to submit accurate information, must be submitted to the CPPA annually.
- *Recordkeeping.* All audit records must be retained for a minimum of five years.

Since audits for certain companies must cover the period beginning January 1, 2027, it is critical that companies begin preparing now to ensure that all required policies and procedures are in place by the end of next year, as those will be subject to review.

Compliance Timeline: Compliance deadlines for conducting audits and submitting certifications are staggered based on annual gross revenue:

- For qualifying large businesses (if annual gross revenue for 2026 is over $ 100 million), the business must complete its first audit by April 1, 2028, for the period covering January 1, 2027 to January 1, 2028;
- For qualifying medium businesses (if annual gross revenue for 2027 is between $50 million to $100 million), the business must complete its first audit by April 1, 2029, for the period covering January 1, 2028 to January 1, 2029; and
- For qualifying small businesses (if annual gross revenue for 2028 was under $50 million), the business must complete its first audit by April 1, 2030, for the period covering January 1, 2029 to January 1, 2030.

Audits must be completed annually thereafter. For each calendar year that an audit is required, the business must submit the accompanying certification on April 1.

3. **Automated Decision-Making Technology (ADMT)**

The finalized ADMT regulations establish comprehensive governance standards for the use of AI and automated tools, focusing on high-stakes decision-making and consumer rights.

Threshold: The ADMT requirements are triggered when a business uses ADMT – defined as "any technology that processes personal information and uses computation to replace human decisionmaking or substantially replace human decisionmaking" – to make a significant decision concerning a consumer. A decision is deemed significant if it results in the denial or provision of (i) financial/lending services; (ii) housing; (iii) education enrollment or opportunities; (iv) employment or independent contracting opportunities or compensation; or (v) health care services.

Key Requirements: Core requirements when the ADMT rules are triggered include:

- Pre-Use Notice: A prominent and conspicuous notice should be provided at or before the point of collection or use of ADMT, detailing among other things the specific purpose for using the ADMT, how the ADMT works, and the consumer's rights.
- Right to Opt Out: Subject to various exceptions, consumers must be provided the ability to opt out of the use of ADMT when the technology is used for a significant decision. One key exception to this requirement is where the business offers the right to appeal an ADMT decision to a human review who has the authority to overturn the decision. Like with other consumer rights under the CCPA, the rules detail how this right and its exceptions should operate.
- Right to Access: Consumers are granted the right to access information about the ADMT's use, with the specific information that should be disclosed outlined in detail in the rules, along with the requirement for how the right should operate.

Compliance Timeline: Businesses that use ADMT to make significant decisions must comply with ADMT consumer rights requirements beginning January 1, 2027. A business that uses ADMT after January 1, 2027, must comply with the relevant rules prior to being implemented.

***

While the compliance deadlines for these rules are staggered, some compliance is required as early as January 1, 2026. And as California has made clear with several high-profile enforcement matters, the state is taking compliance with CCPA rules seriously and actively investigating and pursuing noncompliance. Accordingly, now is the time for organizations to plan and develop strategies to ensure that their compliance approach and overall privacy governance plans account for these new rules.

Wiley's Privacy, Cyber & Data Governance team has helped entities of all sizes from various sectors proactively address risks and compliance with new privacy laws and advocate before government agencies. Please reach out to any of the authors with questions.