

August 06, 2025 | 4 minute read

Still Groundbreaking After Rounds of Tailoring: CCPA Board Finalizes Long-Awaited Regulations on Automated Decision-Making Technologies



Brock Dahl

Partner



Beth George

Partner



Sean Quinn

Counsel

+3 more...

The California Consumer Privacy Act Board (the **Board**) unanimously approved a long-awaited final package of new regulations (the **regulations**) at its July 24, 2025 meeting, imposing significant new requirements on automated decision-making technology (**ADMT**) as well as privacy risk assessments and cybersecurity audit requirements. Given the impact that these regulations will have on businesses, particularly for those using AI, stakeholders have been closely following the development of these regulations. These regulations create obligations related to certain materials that businesses may need to submit directly to the

California Privacy Protection Agency, thus raising the attention that businesses will need to give to these obligations.

We previously discussed a near-final iteration of the proposed regulations. After one last round of minor revisions, the regulations were published for a final public comment period on May 9, and the final version of the regulations passed at the Board's meeting on July 24.

Key Takeaways

- Significant new requirements introduced with respect to ADMT, including new notice requirements and rights for consumers related to ADMT.
- Clarified scope of triggers and content requirements for risk assessments, which as a reminder must be submitted to the California Privacy Protection Agency and contain attestations about the accuracy of the risk assessment.
- Revenue tier-based deadlines for the first annual cybersecurity audits under the new regulations, and enumerated criteria for determining whether such audits are required.

Refined Scope of ADMT Requirements

The final regulations define ADMT as “any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking or substantially replace human decisionmaking.” The regulations also require that a technology substantially *replaces* (not just facilitates) human decision-making to qualify as ADMT. If businesses use a particular technology's output to make a decision without “human involvement” (which is defined under the final regulations), that technology is ADMT, and the regulations' requirements apply to businesses that use it.

Further, certain requirements (including a mandatory risk assessment and consumer notice/opt-out rights) are triggered if ADMT is used to make “significant decisions” concerning consumers. “Significant decisions” are those that involve provision or denial of essential goods and/or services (e.g., financial, housing, employment, healthcare).

Consumer Rights and Notice Requirements Concerning ADMT

The final regulations introduce new consumer rights and notice requirements:

- Businesses must provide plain language explanations of the business purpose, logic, and outputs of ADMT upon request. Further, businesses processing over 10 million consumers’ data annually must publicly report consumer privacy request metrics including total ADMT access requests received, complied with in whole or in part, and denied.
 - Disclosure requirements limit potential over-disclosure by excluding proprietary aspects of ADMT or information that may compromise an individual’s physical safety.
- Businesses must provide “Pre-Use Notice” before making a “significant decision” concerning a consumer using ADMT. Notably, this Pre-Use Notice must include plain language explanation of the specific purpose for which the business plans to use the ADMT and how the ADMT processes personal information to make a significant decision about consumers.
- Consumers may opt out of ADMT usage, but only in cases of “significant decisions.”
 - Some businesses are exempt from opt-out requirements, so long as (i) a human reviewer evaluates ADMT outcomes, and (ii) consumers can appeal ADMT-based decisions.
- Finally, the new regulations prohibit dark patterns and

mandate symmetry in choice to ensure accessibility processes for submitting ADMT access requests and exercising opt-out rights are accessible and not hidden from users.

Mandatory Risk Assessments — Simplified Reporting Process

Under the regulations, companies that engage in data processing activities presenting a “significant risk to consumers’ privacy” must conduct risk assessments *before* engaging in such processing. If a risk assessment determines that risks to consumer privacy outweigh the benefits of processing, that processing is prohibited.

Businesses must undertake risk assessments before:

- Selling or sharing consumers’ data;
- Processing sensitive personal information;
- Using ADMT for “significant decisions” concerning a consumer;
- Training ADMT (i.e., AI) using personal data; and
- Inferring or extrapolating personal attributes in employment or education contexts.

The regulations also introduce documentation and recordkeeping standards. Risk assessment reports must identify and document the types of data being processed (including any sensitive personal information), and reports must be retained for five years after the underlying processing activity ends or until the processing ends, whichever is longer.

Annual Cybersecurity Risk Audits

Businesses must complete annual cybersecurity audits by a qualified, independent professional if they meet specific revenue

and data processing thresholds:

- Processes the data of **250,000 or more** consumers or households;
- Process the *sensitive personal data* of **50,000 or more** consumers; or
- Derive **50% or more of their annual revenue** from selling or sharing personal data;

The final regulations establish deadlines for covered businesses' first annual audits on a tiered basis:

- Businesses with over \$100 million in 2026 gross revenue must complete their first audit by **April 1, 2028** (with the first audit period covering January 1, 2027 through January 1, 2028);
- Businesses with between \$50 million and \$100 million in 2026 gross revenue must complete their first audit by **April 1, 2029** (with the first audit period covering January 1, 2028 through January 1, 2029);
- Businesses with less than \$50 million in 2026 gross revenue must complete their first audit by **April 1, 2030** (with the first audit period covering January 1, 2029 through January 1, 2030).

Conclusion

Businesses may wish to begin efforts to come into compliance with the final regulations given that deadlines for certain obligations are fast approaching, as soon as late 2025 or early 2026. Again, while many commentators were pleased to see certain business-friendly amendments to the proposed version of the regulations compared to prior iterations, these final regulations still create considerable new obligations for businesses to consider and address.

