# The CPPA Finalizes Rules on ADMT, Risk Assessments, and Cybersecurity Audits

18 August 2025
Client Updates

On 24 July 2025, the California Privacy Protection Agency (CPPA) unanimously approved a long-awaited and -debated rulemaking package that addresses: (i) the use of automated decision-making technology, (ii) mandatory risk assessments for high-risk data processing, and (iii) annual cybersecurity audits. The regulations were passed under the California Consumer Privacy Act (CCPA) and now await procedural approval by the California Office of Administrative Law (OAL) within 30 days. Although enforcement will be phased in between 2027 and 2030, covered businesses should begin preparing now to inventory ADMT use cases, identify a cybersecurity audit partner, and develop risk assessment processes.

**Overview of the New Rules**

### A. Automated Decision-Making Technology Rule

The CPPA's first rule governs the use of automated decision-making technology (ADMT) by businesses subject to the CCPA. In particular, where ADMT is used or relied upon in making "significant decisions" about a consumer—such as those affecting access to employment, housing, credit, health care, education, insurance, or essential goods—the business takes on certain obligations.

The definition of ADMT underwent extensive revision throughout the rulemaking process and is ultimately defined as any technology that "replaces or substantially replaces human decision-making" when processing personal information. References to "artificial intelligence" and "behavioral advertising" were removed, but the definition remains broad enough to capture machine learning models, rule-based scoring systems, facial recognition, and even advanced spreadsheets when they materially influence decisions. Certain forms of "extensive profiling" also remain in scope, such as workplace or educational profiling and public-space surveillance.

In the event a business uses ADMT for significant decisions, the business must: (i) provide a detailed pre-use notice of ADMT (which can be included in the standard privacy notice); (ii) offer an opt-out mechanism for ADMT unless a limited exception applies (e.g., providing a method to appeal the automated decision to a human reviewer with authority to overturn); and (iii) furnish additional individualized information about its ADMT use upon request (e.g., about the ADMT logic, ADMT output, how outputs are used in the decision making process).

### B. Risk Assessment Rule

The CPPA's second rule requires businesses to conduct written risk assessments before undertaking certain high-risk data processing activities, including: (i) selling or sharing personal information; (ii) processing sensitive personal information; (iii) using ADMT for significant decisions; (iv) training ADMT to identify, infer traits, or analyze emotion or facial recognition; and (v) automatically processing to infer traits related to an individual's employment, educational, or sensitive location. The risk assessment must identify the purposes, benefits, reasonably foreseeable risks, and proposed safeguards related to the processing, as well as to operational elements like collection process, retention periods, number of consumers impacted, and disclosures made to consumers. Businesses must submit all risk assessments to the CPPA by April 2028 (for assessments conducted in 2026 and 2027) or April of the following year (for assessments conducted in 2028 onward).

### C. Cybersecurity Audit Rule

The third primary rule establishes that any CCPA-bound business whose data processing could pose "significant risk to consumers' security" must complete an independent cybersecurity audit annually. Audits must be based on evidence rather than mere management attestations and conducted by a qualified, objective, and independent professional (who may be external or internal, but if internal, they must not be responsible for the cybersecurity program). The audit must test controls across enumerated areas such as multi-factor authentication, encryption, access management, vulnerability testing, incident response, and vendor oversight. Companies may leverage audits prepared for another purpose under existing frameworks (e.g., NIST CSF 2.0, SOC 2 Type II, ISO 27001) so long as scope and independence requirements are met.

Following completion of each annual cybersecurity audit, a senior executive (or designated board member for public companies) must certify completion and such certification must be filed with the CPPA by staggered deadlines based on the business' annual revenue. Audit supporting documents must be maintained for at least five years.

**Key Compliance Deadlines**

| Requirement | Deadlines |
|---|---|
| Automated Decision-Making Technology | In compliance by **January 1, 2027** |
| Risk Assessments | Start conducting upon effective date<br>First filings due by **April 1, 2028** |
| Cybersecurity Audit<br>(annual revenue > $100 million) | First audit conducted and certification filed by **April 1, 2028** (for FY 2027) |
| Cybersecurity Audit<br>(annual revenue $50–100 million) | First audit conducted and certification filed by **April 1, 2029** (for FY 2028) |
| Cybersecurity Audit<br>(annual revenue < $50 million) | First audit conducted and certification filed by **April 1, 2030** (for FY 2029) |

*Note: Dates assume OAL approval in 2025; statutory text allows minor administrative shifts.*

**Practical Implications and Recommendations**

The CPPA's message is clear: written policies alone are now insufficient. Companies must demonstrate that they have operationalized such policies via technical and organizational safeguards, and that those safeguards operate effectively and can withstand independent audit. Companies should take the following actions to practically prepare as the new rules to come into effect:

1. Establish an ADMT Inventory
   Businesses leveraging vendor-provided or internally-built customer scoring tools, recruiting platforms, or analytics databases may be surprised to find many of those captured by the broad definition of ADMT. Establish a cross-functional team (privacy, IT, HR, product, procurement) to catalogue all existing and planned technologies that substantially supplement or replace human decision-making. Additionally, for each ADMT use case, map the data flows and decision points which will inform the content of future required ADMT disclosures and consumer requests responses.
2. Develop a Risk Assessment Framework
   California's risk assessment rule for high-risk data processing activities largely aligns with the risk assessment requirements found in other privacy laws. Leverage existing data protection impact assessment (DPIA) or legitimate impact assessment (LIA) templates where available but ensure California-specific elements are captured. Schedule periodic reviews every three years or upon material change in processing and integrate risk assessments into the product development lifecycle.
3. Ensure Cybersecurity Audit Readiness
   Begin by benchmarking your business' current cybersecurity program against recognized standards (e.g., NIST CSF 2.0, SOC 2 Type II, ISO 27001). Close gaps in areas expressly called out by the new rules, such as multi-factor authentication, encryption key management, incident response, and vendor oversight. Identify and engage qualified, independent auditors early to reserve capacity and align on scope.
4. Build Out ADMT Consumer-Facing Processes
   The ADMT rule requires various consumer-facing processes that are new but familiar, including pre-use notices, opt-out mechanisms, appeal mechanisms, and consumer request responses. Begin drafting modular plain-language ADMT notices that can be plugged into existing CCPA Privacy Notices at Collection. Build or adapt

existing opt-out workflows already used for the sale/share or personal information or limited use of sensitive personal information. Consider whether existing data subject access request (DSAR) workflows can be extended to ADMT consumer requests or whether separate channels are warranted.

5. Update Internal Policies and External Contracts
   Update corporate policies and protocols to reflect compliance with the new rules, such as protocols for removing consumers from ADMT systems, conducting risk assessments during product development, and furnishing system access during cybersecurity audits. Maintain documentation necessary to rely on any exceptions (e.g., human appeal exception to ADMT opt-out mechanism). Because businesses remain liable for the ADMT and data processing activities of vendors, update vendor agreements to require cooperation with your business' new obligations.
6. Educate Stakeholders and Secure Budget
   Board-level attention is now essential. Brief executive leadership and the board on upcoming regulatory obligations, certification filings, and potential enforcement exposure. Incorporate compliance milestones into budget planning to account for audit costs, new tools, increased headcount, and additional privacy engineering resources.

**Conclusion**

The CPPA's latest rules on ADMT, cybersecurity audits, and risk assessments represent a decisive shift from simple notice-and-choice privacy toward more mature, operationalized, and evidence-based technology governance. While the phased deadlines provide some runway, the operational lift—especially for global enterprises leveraging a sophisticated system of algorithms and tools—could be substantial. By acting now to inventory ADMT, institutionalize risk assessments, and identify cybersecurity audit partners, businesses can mitigate regulatory risk, build consumer trust, and ultimately strengthen the resiliency of their data ecosystems.

Feel free to reach out to any member of our Privacy & Cybersecurity team for more tailored guidance regarding your business' specific risk profile and strategic compliance roadmap.

**ABOUT BAKER BOTTS L.L.P.**
*Baker Botts is an international law firm whose lawyers practice throughout a network of offices around the globe. Based on our experience and knowledge of our clients' industries, we are recognized as a leading firm in the energy, technology and life sciences sectors. Since 1840, we have provided creative and effective legal solutions for our clients while demonstrating an unrelenting commitment to excellence. For more information, please visit* ***bakerbotts.com****.*

**Related Professionals**

**Matthew R. Baker**

Partner

**Justin Bryant**

Associate

**Michelle N. Molner**

Senior Associate