July 28, 2025

CPPA Board Adopts CCPA Regulations on ADMT, Risk Assessments, Cybersecurity Audits and Reopens Public Comment on DROP Requirements

by Meghan K. Farmer , Tatum Andres

On July 24, 2025, the California Privacy Protection Agency (CPPA) Board held a public meeting to finalize major amendments to the CCPA regulations, including rules on Automated Decision-Making Technology (ADMT), risk assessments, cybersecurity audits, and insurance companies. However, the Board opted to revisit the Delete Request and Opt-Out Platform (DROP) regulations, reopening those rules for further public input

Key Highlights

1. Adoption of CCPA Regulations on ADMT, Risk Assessments, and Cybersecurity Audits.

The CPPA unanimously approved regulations that expand the rules' focus from the CCPA's core scope of consumer privacy to also regulate cybersecurity and AI decision-making.

Automated Decision-Making Technology (ADMT)

- Compared with the first draft of the regulations, the definition of ADMT was narrowed in the final version to cover systems that "substantially replace" human decision-making.

- The scope of consumer opt-out rights was also reduced. The original draft had included broad opt-out rights for uses like profiling for behavioral advertising (which can include first party advertising) and hiring. The new version excludes many of these categories like workplace profiling, the training of ADMT systems, and certain advertising.

Cybersecurity Audits

- A business subject to the CCPA must complete an independent cybersecurity audit if the business' processing of personal information could pose a significant risk to consumer security. However, under the new final version of regulations, businesses can rely on audits conducted for other purposes, as long as they meet the necessary criteria under the CCPA.

- Businesses that must complete cybersecurity audits under the CCPA must complete them every year and submit a certification of completion to the CPPA for each year. The new final version of the regulations clarified who is authorized to submit the annual certification of completion and what specific information that certification must contain.

- The final regulations also adjusted deadlines for cybersecurity audits based on business revenue thresholds. For instance, businesses with over $100 million in annual revenue may face a January 1, 2028, deadline; smaller businesses may have until January 1, 2030.

Risk Assessments

- In the earlier version of the regulations, businesses were required to conduct and submit risk assessments to the CPPA before starting certain types of personal data processing, provided they met specific thresholds. The new final regulations have relaxed some of these requirements. Notably, businesses implementing ADMT no longer need to include in their risk assessments detailed explanations of the steps taken to maintain the quality of personal information processed by ADMT. Previously, "quality of information" was defined to cover the completeness, representativeness, timeliness, validity, accuracy, consistency, and reliability of the personal information for the business's proposed use of ADMT. Removing this obligation significantly reduces the amount of information businesses must include in their assessments.

The finalized rules will now be reviewed by the California Office of Administrative Law, which has 30 days to confirm compliance with procedural requirements.

2. DROP Regulations Reopened for Public Comment

The CPPA declined to adopt the DROP regulations in their current form, instead reopening them for public input with several proposed changes including:

Suppression List Requirements

- Data brokers must delete all personal data associated with a DROP request, including inferred data.A minimal suppression record may be retained to prevent repopulation.

- Brokers may now share suppression lists with contractors and service providers to ensure continued compliance.

California Residency Verification

- Originally, consumers might have had to verify their residency with the CPPA before submitting a DROP request.

- The updated proposal places the full responsibility on the CPPA to verify requester's residency. Once verified, brokers must process the request accordingly.

The public comment period for these revised DROP regulations will remain open for 15 days. Businesses and stakeholders are encouraged to submit feedback to help shape the final version.

Questions? Our Privacy Team is available to assist: Cybersecurity, Privacy & Data Governance