Stay Current

PAUL HASTINGS

October 2025

Follow us on LinkedIn

Regulatory Update

Long-Awaited CCPA Regulations Take Major Step Toward Effectiveness

By Aaron Charfoos, Michelle A. Reed, Rachel Kurzweil and Jeremy Berkowitz

Businesses that are already subject to the California Consumer Privacy Act (CCPA) will soon have a host of new regulatory requirements to comply with. On Sept. 23, the California Privacy Protection Agency (CPPA) announced that the California Office of Administrative Law (OAL) approved the CPPA's long-awaited regulations on cybersecurity audits, risk assessment, automated decision making and other updates to the existing regulations.

While covering various topics, the new regulations particularly focus on (1) businesses' use of automated decision-making technologies (ADMT); (2) requirements for conducting risk assessments, and (3) requirements for conducting cybersecurity audits. With OAL's review complete, these regulations officially become effective on Jan. 1, 2026. However, as the CPPA noted, businesses have some additional time to comply with these new requirements.

Automated Decision-Making Technology

The regulations require that by Jan. 1, 2027, businesses using ADMT for significant decisions provide notice of such use at *or before point of collection.* These notices must clearly state the specific purpose for which businesses plan to use ADMTs and not rely on generic terms. Pre-use notices must also provide additional information about how ADMT makes a significant decision and how a significant decision would be made if a consumer opts out of the ADMT. Consumers will have the right to *opt out* of such uses of ADMT, subject to limited exceptions, and to access information about how the ADMT works.

The CCPA specifically defines ADMT as follows:

- ADMT is defined as "technology that processes personal information and *replaces or substantially replaces human decision-making*; "Substantially replace" means using the output of the ADMT without human involvement in making the decision.

- A significant decision is defined as "those relating to financial/lending services, housing, educational enrollment or opportunities, employment or contracting, compensation, or health care services."

Risk Assessments

The new regulations require that businesses conduct a risk assessment before initiating any processing activity that involves a "significant risk." Businesses must also submit the following information about risk assessments to the CPPA: (a) point of contact; (b) period covered (month and year); (c) number of risk assessments conducted or updated during the period that the submission covers; (d) the categories of personal information and sensitive personal information that the assessments cover; (e) an attestation that the business has completed the required risk assessment; and (f) the name and business title of the person submitting the risk assessment information and the date of the certification. Businesses conducting risk assessments in 2026 and 2027 must submit this information by April 1, 2028. Assessments conducted after 2027 will be due by April 1 of the following year.

The regulations provide that significant risks can include activities such as:

- selling or sharing personal information;
- processing sensitive personal information, including financial or account credentials, health/genetic data, precise geolocation, etc.;
- using ADMT to make significant decisions; or
- using automated processing to infer consumer traits or behavior (e.g., profiling, emotion or facial recognition, traits based on sensitive locations, job/study/employment status) even if not yet used for a final decision. Training of ADMT systems in those contexts is also a trigger.

If companies engage in such processing, they are required to complete risk assessments before starting the processing activity. If there is a material change to the processing activity, the assessment must be updated within 45 calendar days of that change. Even absent a change, assessments must be reviewed and updated at least once every three years.

The regulations contain significant information on what each risk assessment must provide including details on the processing and related protections such as:

- purposes of the processing activities;
- categories of personal information involved;
- operational details of how the processing is done;
- number of consumers affected by the processing;
- retention of personal information;
- what notice is provided to customers about the processing activities;
- names or categories of service providers, contractors or third parties to whom personal information is disclosed to or made available and the purposes for disclosure;
- risk-benefit analysis for conducting the processing, including potential ramifications to customers;
- safeguards the business plans to implement;
- document whether the business will initiate the processing subject to the risk assessment;

- identify individuals that provided information for the risk assessment (legal counsel excluded); and

- the date the assessment was reviewed and approved (legal counsel excluded) and names of those who approved it.

Cybersecurity Audits

Businesses whose processing of consumer personal information presents a "significant" risk to consumers' security must conduct an *annual* cybersecurity audit. The regulations specify that businesses that meet any one of the following thresholds are required to complete the cybersecurity audit:

- Derive at least 50% of their annual revenue from selling or sharing personal information for targeted advertising purposes.

- Process personal information of at least 250,000 consumers in a calendar year.

- Process sensitive personal information of at least 50,000 consumers in a calendar year.

Audits must be conducted by either an external party or an internal auditor who does not report to an individual with responsibility for managing the cybersecurity program. While the regulations set out specific components of what the audit must cover, generally such audits must assess how a business's cybersecurity program protects personal information from unauthorized access, destruction, use, modification or disclosure and protects against unauthorized activity resulting in the loss of availability of personal information. For example, the regulations specify that the audit must: (1) describe the business's information systems including policies and procedures the audit assessed, criteria used for the audit and evidence examined; (2) the cybersecurity controls used by the business, how they are implemented and their effectiveness; (3) any noted gaps or weaknesses in the program; and (4) how the business plans to address the weaknesses.

The audit must also identify those responsible for the cybersecurity program, the auditor and their qualifications and include a signed statement by the "highest-ranking auditor" that they completed an independent review of the business's cybersecurity program and information system, exercised objective and impartial judgment on all issues within the scope of the cybersecurity audit and did not rely primarily on assertions or attestations by the business's management.

Upon completion of each audit, businesses must submit a written certification to the CPPA attesting that the audit has been finalized in accordance with the regulations.

Notably, the regulations provide that businesses can utilize assessments or audits prepared for other purposes provided that they meet the requirements of the regulations either on their own or through supplements.

Businesses are required to start conducting cybersecurity audits based on their revenue. A business with gross revenue over $100 million in 2026, must complete and submit an audit to the CPPA by April 1, 2028, covering the period from Jan. 1, 2027, through Jan. 1, 2028. A business with gross revenue over $50 million in 2027, must complete and submit an audit by April 1, 2029, covering the period from Jan. 1, 2028, through Jan. 1, 2029. A business with gross revenue under $50 million in 2028, must complete and submit an audit by April 1, 2030, covering the period from Jan. 1, 2029, through Jan. 1, 2030.

Next Steps

Given these new rules and timelines, here are steps businesses should be looking to take now:

1. **Understand your use of ADMT / automated decision-making:** Identify where in your operations you use or plan to use systems that make or substantially replace human decision-making in significant decisions.

2. **Review data flows and risk exposures:** Determine the sensitivity of personal information processed, especially sensitive personal information or neural data, and assess risk of harm and likelihood of impacts, particularly in high-risk contexts.

3. **Update notice, opt-out, and transparency mechanisms:** Build or refine your disclosure protocols (point of collection, privacy policies, etc.) to ensure they meet ADMT requirements; set up mechanisms for consumer opt-out and access to explanation of logic.

4. **Plan for risk assessments:** Assess whether your business will need to conduct risk assessments, ensure that your compliance programs meet all of the CCPA requirements and plan ahead to ensure that you can remediate any additional risks.

5. **Plan for cybersecurity audits:** Assess whether your business meets the thresholds now or will soon and then assess your compliance program. There is still time to fill in any gaps before you are audited.

The Paul Hastings Data Privacy and Cybersecurity practice is closely monitoring these developments. If you have any questions, please do not hesitate to contact any member of our team.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Chicago

Aaron Charfoos
+1-312-499-6016
aaroncharfoos@paulhastings.com

Dallas

Michelle A. Reed
+1-972-936-7475
michellereed@paulhastings.com

Washington D.C.

Rachel Kurzweil
+1-202-551-1940
rachelkurzweil@paulhastings.com

Jeremy Berkowitz
+1-202-551-1230
jeremyberkowitz@paulhastings.com