Skadden

Cybersecurity and Data Privacy Update

October 3, 2025

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

320 S. Canal St.
Chicago, IL 60606
312.407.0700

1440 New York Ave., NW
Washington, DC 20005
202.371.7000

California Finalizes CCPA Regulations for Automated Decision-Making Technology, Risk Assessments and Cybersecurity Audits

Executive Summary

- **What's new:** Regulations under the California Consumer Privacy Act (CCPA) are finalized, establishing a comprehensive regulatory framework for businesses using California consumers' information, including those employing automated decision-making technology (ADMT) for "significant decisions."
- **Why it matters:** The regulations, which begin to come into effect January 1, 2026, mandate: consent and opt-out procedures; detailed disclosures about privacy policies and the ADMT process; risk assessments; and cybersecurity audits. The new regime significantly reshapes governance requirements for businesses that process the personal information of California consumers.
- **What to do now:** Companies will want to begin mapping current and planned uses of ADMT, identifying processing activities that may trigger risk assessments, and prepare for possible cybersecurity audits.

On September 23 2025, the California Office of Administrative Law approved the California Privacy Protection Agency's (CPPA's) regulations under the California Consumer Privacy Act (CCPA). The final regulations create three new areas of compliance under the CCPA:

- Obligations for businesses that use automated decision-making (ADMT) for "significant decisions" about California consumers.
- Mandatory risk assessments for certain high-risk processing activities.
- Annual cybersecurity audits for businesses meeting specified thresholds.

While these requirements are phased in over several years, they represent a significant expansion of the CCPA's reach and will require businesses to undertake new documentation, governance and consumer-facing processes.

They also clarify existing regulations, most notably:

- Where consent is required for a processing purpose, individuals must be able to withdraw such consent at any time.
- Links to privacy policies must appear not just on the business's homepage, but on any web page where personal information is collected.
- Opting out must be as easy as opting in.
- Access requests can be for information beyond the preceding 12 months.

California Finalizes CCPA Regulations for Automated Decision-Making Technology, Risk Assessments and Cybersecurity Audits

Automated Decision-Making Technology (ADMT)

The regulations impose requirements on business that use ADMT to make a "significant decision" concerning a consumer. The regulations narrowly define ADMT as technology that: (1) processes personal information and (2) uses computation to *replace or substantially replace* human decision-making. "Significant decisions" includes decisions that affect finances, housing, education, employment or health care, but not advertising (which was included in previous drafts of the regulations).

Beginning April 1, 2027, businesses using ADMT for significant decisions must:

- Conduct a risk assessment.
- Provide a pre-use notice to consumers about the business's use of ADMT for a significant decision.
- Provide an opt-out option to California consumers, subject to certain exceptions.
- Allow consumers to request access to information about the business's use of ADMT, including information about the logic of the ADMT and how ADMT outputs are used in decision-making.
- Provide California consumers with the ability to appeal the results of ADMT.

Risk Assessments

Businesses subject to the CCPA must conduct and maintain risk assessments before initiating processing activities that pose "significant risk" to consumer privacy. Triggering activities include:

- Selling or sharing personal information for cross-context behavioral advertising purposes.
- Processing sensitive personal information.
- Using ADMT for a significant decision concerning a consumer.
- Profiling a consumer in certain education and employment contexts.
- Profiling a consumer based on their presence at a sensitive location.
- Processing the personal information of consumers, which the business intends to use to train an ADMT for a significant decision concerning a consumer.
- Processing personal information of consumers to 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.

Risk assessments will need to evaluate "negative impacts" on consumers, such as discrimination, economic or physical harm, reputational harm, or interference with consumers' ability to make informed choices.

Businesses can conduct a single risk assessment for a comparable set of processing activities (*e.g.*, similar processing activities that present similar risks to consumers' privacy). Businesses can also leverage risk assessments conducted for other purposes (*i.e.*, pursuant to a requirement under the EU's General Data Protection Regulation), provided that the risk assessment contains the information that must be addressed under the CCPA regulations. Businesses must retain assessments for the duration of processing or five years after completion.

For processing activities already underway, initial assessments are due by December 31, 2027. For risk assessments conducted in 2026 and 2027, businesses are required to submit information regarding the assessment — but not the assessment itself — to the CPPA by April 1, 2028. Businesses must include the following in their submission: a designated contact, the time period covered by the submission, the number of risk assessments conducted during that period, an indication of whether the risk assessments addressed the processing of personal information under the CCPA, an attestation, and the name of the individual submitting the report.

Cybersecurity Audits

Businesses subject to the CCPA will be required to conduct independent annual cybersecurity audits, covering core components of their cybersecurity programs, if their processing presents a "significant risk" to the security of California consumers. A "significant risk" to consumers' security exists where a business:

- Derives 50% or more of its annual revenue from selling or sharing personal information (which also represents one of the thresholds for CCPA applicability); or
- Derives annual gross revenue over $25 million and processes either:
  - Personal information of at least 250,000 consumers; or
  - Sensitive personal information of at least 50,000 consumers.

Audits must be performed by a qualified, objective, independent professional (either internal or external) using recognized auditing standards. Businesses must generate a detailed audit report describing the business' cybersecurity program, including security measures and policies, as well as the business' information systems, evidence examined and audit findings. The business must submit a certification of completion by the auditor to the CPPA each year that the business is required to conduct a cyber audit. All audit-related records must be retained for at least five years.

California Finalizes CCPA Regulations for Automated Decision-Making Technology, Risk Assessments and Cybersecurity Audits

The annual audit requirements will be phased in based on revenue, with the first audits due on the following schedule:

- **April 1, 2028:** Businesses with more than $100 million in 2026 revenue.
- **April 1, 2029:** Businesses with $50 million to $100 million in 2027 revenue.
- **April 1, 2030:** Businesses with less than $50 million in 2028 revenue.

Steps To Prepare

The CPPA's finalized regulations mark a sharp change in California's privacy regime, bringing ADMT oversight, formal risk assessments and independent cybersecurity audits onto the compliance landscape. With phased deadlines approaching in 2027, businesses will need to consider what steps to take proactively to be ready for compliance.

In particular, companies should consider:

- Evaluating ADMT usage by inventorying current and planned ADMT tools, particularly in hiring, lending, fraud detection or customer profiling.
- Preparing for risk assessments by developing frameworks and templates now to assess and document high-risk processing activities.
- Proactively reviewing cybersecurity programs against the core components that cybersecurity audits will be required to address.
- Reviewing consumer-facing materials and preparing to revise notices and data subject rights processes to meet the new requirements.

Contacts

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Dana E. Holmstrand
Associate / Washington, D.C.
202.371.7014
dana.holmstrand@skadden.com

Lisa V. Zivkovic
Associate / New York
212.735.2887
lisa.zivkovic@skadden.com

Sammuel Kim
Associate / Washington, D.C.
202.371.7301
sammuel.kim@skadden.com