

California approves privacy rules on automated decisions, risk assessments and audits

Source copy kept by wheresthe.ai for the story "California approves privacy rules on automated decisions, risk assessments and audits" (<https://wheresthe.ai/d/us-ca-cppa-admt-regulations-approved-2025-09/>).

Source: <https://connectontech.bakermckenzie.com/new-california-requirements-on-ai-risk-assessments-and-cybersecurity-cppa-adopts-expanded-regulations/>

Text saved 18 Oct 2026 (the page as published).

SHA-256 of the saved text: f9eee1b6d7be5f3cd07529f313fc7055afc83dd0dc9c09a3327f4a22c90240c4

Documents the source offers: https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_mod_txt_pro_reg.pdf; <https://oag.ca.gov/sites/all/files/agweb/pdfs/db/2016-data-breach-report.pdf>

Share

Share on Twitter

LinkedIn

Email

UPDATE: On September 23, 2025, the California Office of Administrative Law approved the CPPA's draft regulations. The regulations will take effect on January 1, 2026. The CPPA is considering additional amendments to the regulations that may be published in future drafts.

On July 24, 2025, the California Privacy Protection Agency (CPPA) took a step forward in rulemaking under the California Consumer Privacy Act (CCPA) by adopting regulations governing automated decision-making technology, risk assessments, and cybersecurity audits. The CPPA proposed rules in early 2023 and the version adopted this week was revised in May 2025.

The CPPA board voted 5-0 to adopt the regulations and authorized staff to submit the final rulemaking package to the Office of Administrative Law (OAL). The OAL has 30 working days to process and approve the regulations, at which point the rules will take effect.

With this approval, the CPPA has fulfilled its mandate under Proposition 24 to clarify and expand the CCPA by creating enforceable rules governing automated decision-making technology and requiring cybersecurity audits and risk assessments. Under the Regulations, "Automated decision-making technology" or "ADMT" means any technology that processes personal information and uses computation to execute a decision, replace human decision-making, or substantially replace facilitate human decision-making.

The CPPA Board emphasized that while this action marks an implementation milestone, they expect the regulations to evolve over time. "One of the benefits of regulations . . . is that they are more changeable than statutes tend to be" said CPPA Chair Jennifer Urban. "We need to have the regulations in place in order to move forward, but we will be taking in more information as time goes on."

What the Regulations Cover

The adopted rules address three main areas:

Automated Decision-making Technology (ADMT)

As of January 1, 2027, businesses have to notify individuals about the use of ADMT for "significant decisions," allow them to opt out of these use cases, entitle them to access information on how decisions were made, appeal decisions, and conduct risk assessments (risk assessments are discussed further below).

"Significant decisions" include any decision that "results in the provision or denial of financial or lending services, housing, education enrollment or opportunities, employment or independent contracting opportunities or compensation, or healthcare services." (In the final rules, behavioral advertising no longer triggers ADMT-related requirements).

Risk Assessments

Organizations engaging in high-risk data processing must conduct and submit assessments evaluating the necessity, proportionality, and potential impact of their data practices.

The CCPA or the Attorney General may require a business to submit its risk assessment reports to the CCPA or to the Attorney General at any time.

The following activities pose “significant risks” that require assessments:

“Selling” or “sharing” personal information;

Processing “sensitive personal information,” except for employment-related purposes like compensation, benefits, or legal compliance.

Using ADMT to make significant decisions about a consumer;

Using automated processing to infer or extrapolate personal traits (e.g., intelligence, health, behavior) based on a consumer’s activity as an employee, student, or applicant;

Using automated processing to infer or extrapolate a consumer’s traits based on their presence in a sensitive location (healthcare facilities; pharmacies; domestic violence shelters; food pantries; housing/emergency shelters; educational institutions; political party offices; legal services offices; union offices; and places of worship), unless the information is used only to deliver goods or provide transportation;

Using personal information to train ADMT or identity-verification technologies (e.g., facial or emotion recognition).

Examples of when a business must conduct a risk assessment include:

Using ADMT, such as emotion-recognition tools, to make significant decisions about individuals—like hiring—without human involvement.

Disclosing sensitive personal information, such as geolocation, ethnicity, or medical data, to third parties, especially when that information was provided for personal or intimate purposes.

Targeting consumers with advertisements based on profiling from personal or financial information, particularly when the profiling infers traits like interests, preferences, or reliability.

Extracting and using biometric data, such as faceprints from photographs, to train facial-recognition or similar identity-verification technologies

Cybersecurity audits

A business subject to CCPA whose processing of personal information presents a “significant risk” under the statute must complete annual cybersecurity audits documenting how these risks are mitigated with security controls and processes. Companies must submit annual written certifications to the CCPA that the business has completed the cybersecurity audit. Companies do not have to submit the actual audit report, but can expect demands to see the report by the CCPA, California Attorney General, and plaintiffs in lawsuits following data security breaches.

“Significant risk” that trigger cyber audit requirements means the business either:

had annual gross revenues in excess of twenty-five million dollars (\$25,000,000) in the preceding calendar year (inflation adjusted) and, in the previous calendar year, processes the personal information of 250,000 Californians or the sensitive personal information of 50,000 Californians; or

derives 50 percent or more of its annual revenues from selling or sharing consumers’ personal information.

If a business subject to the CCPA generates more than \$100 million revenue in 2026, their first audit will be due by April 1, 2028. If it makes between \$50 million and \$100 million in 2027, the audit is due by April 1, 2029. If it makes less than \$50 million in 2028, the audit is due by April 1, 2030.

After April 1, 2030, all businesses subject to the CCPA whose processing constitutes a significant risk must conduct a cybersecurity audit and file its certification of completion with the CCPA by April 1 of the following year.

The draft cyber audit regulations would still require businesses to assess and document how the business’ cybersecurity program protects personal information from unauthorized access, destruction, use, modification, or disclosure; and protects against unauthorized activity.

The regulations list numerous data security measures in §7123(c) that businesses need to consider for purposes of satisfying their obligation under California law to maintain reasonable security measures, including multifactor authentication (MFA); strong passwords; encryption of personal information at rest and in transit; account management and access controls; taking inventory of data flows, hardware, and software; secure configuration; patch management; vulnerability scanning; logging; and training. Businesses are not explicitly required to implement all these and other listed requirements, but would have to explain to a regulator, plaintiff, insurance company, auditor, or others after a breach or during an investigation why the business did not implement a certain requirement if it could have helped to prevent the breach. Businesses should therefore consider the listed requirements as a roadmap, as with respect to “addressable” requirements under HIPAA and requirements listed in guidance from the FTC and regulators in the past, including California’s Attorney General in its 2016 breach report .

The regulations add other significant new requirements to the CCPA privacy regime. To ensure compliance under the new regulations, businesses subject to CCPA are encouraged to take the following steps:

Identify all technologies that use automated decision making technology and conduct appropriate risk assessments. Pay particular attention to AI-enabled technologies or higher risk technologies that support HR use cases in recruiting, hiring, applications, succession planning, monitoring, etc.

Create or update risk assessments that leverage existing frameworks and assessments for InfoSec and privacy.

Update its CCPA governance documents to include processes that comply with the new regulations.

Update public facing disclosures to comply with new regulations.

Configure privacy enhancing technologies to provide opt-out rights where required under new regulations.

Work with its InfoSec team to conduct readiness assessments in anticipation of mandatory audits. Readiness assessments can help businesses identify gaps in “reasonable security” that can be remediated long before the mandatory audits take effect.

Train its workforce on the new data, privacy and cyber laws and regulations in the jurisdictions you operate.

See Baker McKenzie’s earlier coverage of the draft regulations here: [Off to the Races: California Advances CCPA Regulations on Cyber, Risk & AI – Connect On Tech](#)

Categories:

AI

Cyber

Tags:

California CPPA Data Privacy & Security

Author Cynthia Cole

Cynthia J. Cole is a partner in Baker McKenzie’s Commercial, Technology and Transactions and Data and Cyber practices, and co-chair of Baker Women California. A former CEO and General Counsel, just before joining the Firm, Cynthia was Deputy Department Chair of the Corporate Section in the California offices of Baker Botts where she built the technology transactions and data privacy practice. An intellectual property transactions attorney, Cynthia also has expertise in AI, digital transformation, data privacy, and cybersecurity strategy.

Website

Author Justine Phillips

Justine focuses her practice on both proactive and reactive cybersecurity and data privacy services, representing clients in matters related to information governance, diligence in acquisitions and investments, incident preparedness and response, the California Consumer Privacy Act, privacy litigation, and cyber litigation.

Website

Author Helena Engfeldt

Helena practices international commercial law with a focus on assisting and advising technology companies with cross-border transactions, drafting and negotiating commercial agreements, and advising on global data privacy law compliance. Helena also advises software developers, e-commerce companies, and global mobile and web gaming developers on regulatory restrictions, intellectual property, contracting and data privacy.

Website

Author Lothar Determann

Lothar has been helping companies in Silicon Valley and around the world take products, business models, intellectual property and contracts global for nearly 20 years. He advises on data privacy law compliance, information technology commercialization, interactive entertainment, media, copyrights, open source licensing, electronic commerce, technology transactions, sourcing and international distribution at Baker McKenzie in San Francisco & Palo Alto.

Website

Author Jonathan Tam

Jonathan Tam is a partner in the San Francisco office focused on global privacy, advertising, intellectual property, content moderation and consumer protection laws. He is a qualified attorney in Canada and the U.S. passionate about helping clients achieve their commercial objectives while managing legal risks. He is well versed in the legal considerations that apply to many of the world's cutting-edge technologies, including AI-driven solutions, wearables, connected cars, Web3, DAOs, NFTs, VR/AR, crypto, metaverses and the internet of everything.

Website

Author Garrett Stallins

Garrett is an associate in Baker McKenzie's North America Intellectual Property Group and is based in our San Francisco office. His practice focuses on helping clients build effective information governance programs, comply with privacy laws and regulations, and respond to cybersecurity incidents.

Website

Related Posts

Egypt: Personal Data Protection Law Update

October 8, 2026

Thought for the week: AI agents raise new cybersecurity and liability questions

October 5, 2026

The future of the ICO – governance changes and draft corporate strategy signal key regulatory priorities

September 28, 2026