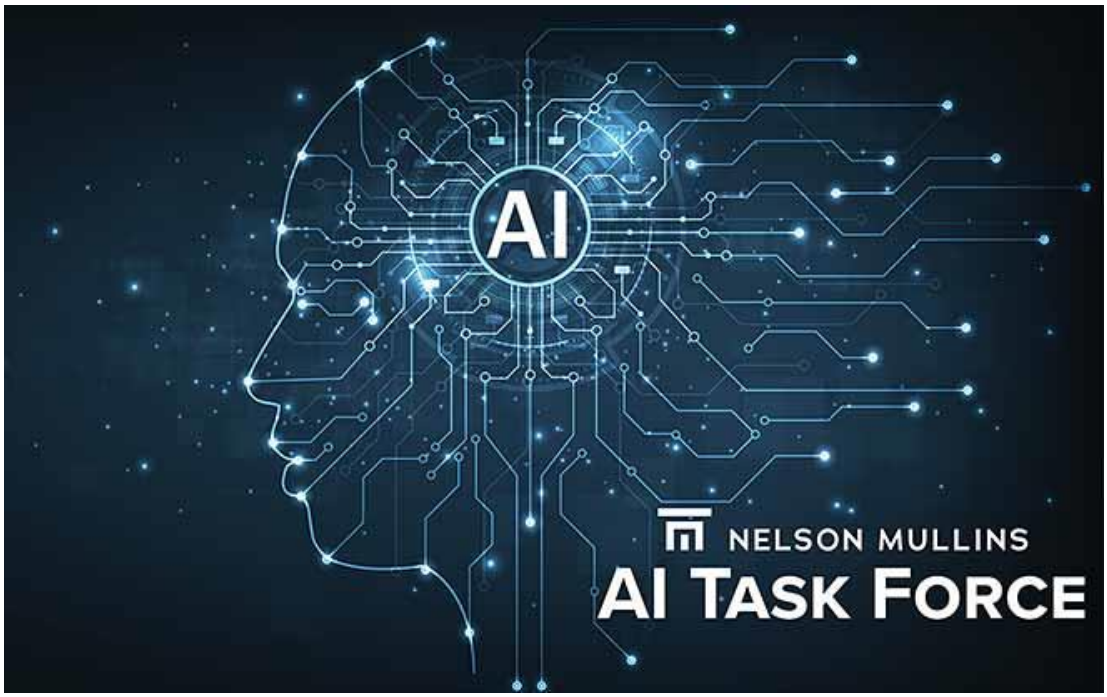
NELSON MULLINS



July 29, 2025

California Finalizes CCPA Regulation Amendments: New Compliance Obligations for Cybersecurity, Risk Assessments, and Automated Decision-Making

By Mallory Acheson, CIPM, CIPP/E, FIP, Jennie Cunningham, Amanda Witt

This is part of a series from Nelson Mullins' AI Task Force. We will continue to provide additional insight on both domestic and international matters across various industries spanning both the public and private sectors.

On July 24, 2025, the California Privacy Protection Agency (CPPA) Board approved a final package of amendments to the regulations implementing the California Consumer Privacy Act (CCPA). These sweeping changes impose substantial new compliance obligations on businesses operating in California, particularly in the areas of cybersecurity audits, data protection risk assessments, and automated decision-making technology (ADMT).

The amended regulations—designed to reinforce consumer protections, improve accountability, and guide the responsible use of emerging technologies—introduce complex, multi-phase requirements that begin taking effect in 2027. The final rules now proceed to the California Office of Administrative Law (OAL) for procedural approval.

Key Regulatory Updates

1. Mandatory Annual Cybersecurity Audits

For the first time, the regulations require annual, independent cybersecurity audits for businesses that meet specific risk-based thresholds. These include:

- Deriving 50% or more of annual revenue from selling or sharing personal information; or
- Annual gross revenue over $25 million (adjusted for inflation) and processing either:
  - Personal information of at least 250,000 consumers, or
  - Sensitive personal information of at least 50,000 consumers.

Audit Requirements:

- Must be conducted by qualified, objective professionals (internal or external).
- Must include:
  - Overview of audited systems and data environments;
  - Evaluation of cybersecurity programs aligned with industry standards for "reasonable security";
  - Gap analysis and remediation actions;
  - Breach and incident review for the audit period.
- Internal audit reports must be done by the highest-ranking auditor who reports directly to a member of the business's executive management team who does not have direct responsibility for the business's cybersecurity program.
- The cybersecurity audit report must be provided to a member of the business's' executive management team who has direct responsibility for the business's cybersecurity program.

Compliance Deadlines:

- April 1, 2028 – Businesses with annual revenue over $100 million
- April 1, 2029 – Revenue between $50 million–$100 million
- April 1, 2030 – Revenue under $50 million

Key Takeaway: Businesses must begin establishing audit processes now, including identifying qualified audit personnel, establishing internal reporting lines, and documenting cybersecurity practices comprehensively.

2. Data Protection Risk Assessments for High-Risk Processing

Businesses that engage in data processing activities deemed to present a significant risk to consumers' privacy will be required to conduct and submit formal risk assessments. Activities triggering this requirement include:

- Selling or sharing personal information;
- Processing sensitive personal information;
- Using ADMT for significant decisions;
- Profiling individuals using automated inferences in employment, education, or sensitive location contexts;

- Using consumer data to train ADMT or systems involving facial/emotion recognition or identity verification.

Risk Assessment Requirements – each assessment must include:

- Detailed description of processing purpose;
- Risk/benefit analysis for consumers;
- Mitigation measures taken;
- Consideration of less intrusive alternatives.

Service providers and vendors should also be prepared to support covered businesses in completing these assessments, potentially through data mapping assistance and impact evaluation.

3. New Governance Obligations for Automated Decision-Making Technology (ADMT)

The final rules significantly expand obligations around the use of ADMT, targeting tools that replace or substantially influence human decision-making in legally or financially significant scenarios. While earlier drafts referred more broadly to "AI," the final rules removed the term to narrowly focus on ADMT (e.g., AI) used in significant decision-making contexts.

Notable Obligations:

- Pre-Use Notices: Before collecting or repurposing data for ADMT, businesses must notify consumers with clear descriptions of intended use.
- Right to Know & Appeal: Consumers must be informed when ADMT is used and given the right to access "meaningful information" about how the system works—including logic, inputs, and outcomes—and appeal decisions.
- Opt-Out Mechanism: A new, separate opt-out link titled "Opt Out of Automated Decisionmaking Technology" is required on websites.
- Opt-In Consent: Required when ADMT is used to process sensitive information or information related to minors.
- Human Review Exception: Exempts ADMT systems where meaningful human oversight or override exists.

Compliance Deadline: January 1, 2027

4. Enhanced Transparency and Documentation Requirements

The amendments significantly enhance transparency expectations related to privacy notices, consumer rights, and internal documentation:

- No More Vague Disclosures: General statements like "to improve services" are no longer sufficient. Businesses must specify the exact categories of data collected and the specific purposes for each.
- ADMT Access Requests: Responses must include:

- Clear explanations of the logic behind the ADMT;
- Description of the system's input/output;
- Information about data sources and assumptions used in modeling.

These requirements aim to ensure consumers receive comprehensible, actionable information about how their data is used and decisions are made.

Recommended Next Steps for Businesses

To prepare for compliance with these newly finalized rules, businesses should begin:

- Reviewing and updating privacy notices to meet new specificity and transparency requirements;
- Conducting internal audits to assess whether cybersecurity audit and risk assessment requirements apply;
- Inventorying and evaluating current and planned ADMT systems, including those used in hiring, benefits eligibility, financial services, or profiling;
- Building governance frameworks for ADMT usage, including consumer-facing tools for opt-out and appeal;
- Engaging service providers and vendors in preparing for collaborative compliance with risk assessment and audit obligations.

Contact Us

Our Global Privacy & Security team is actively advising clients on these regulatory changes and offering:

- Compliance readiness assessments;
- Cybersecurity audit preparation and risk documentation support;
- ADMT governance strategy and technical implementation assistance;
- Targeted training for legal, compliance, and product teams.

To discuss how these changes affect your organization or to request a tailored compliance roadmap, please contact us.

Follow Nelson Mullins' Idea Exchange for more thought leadership from our AI Task Force, or click here to subscribe to emails from the Nelson Mullins AI Task Force blog.

View on Website

NELSON MULLINS

GET IN TOUCH

Mallory Acheson, CIPM, CIPP/E, FIP

Partner

T 615.664.5378

mallory.acheson@nelsonmullins.com

Jason I. Epstein

Partner

T 615.664.5364

jason.epstein@nelsonmullins.com

Daniel C. Lumm, CIPP/US

Partner

T 864.373.2341

daniel.lumm@nelsonmullins.com

Geoffrey P. Vickers

Partner

T 615.664.5321

geof.vickers@nelsonmullins.com

NELSON MULLINS

GET IN TOUCH

Anthony A. Laurentano
Partner
T 617.217.4624
anthony.laurentano@nelsonmullins.com

Franklin Chou
Senior Associate
T 212.413.9035
franklin.chou@nelsonmullins.com

Johnathan H. Taylor
Senior Associate
T 404.322.6339
johnathan.taylor@nelsonmullins.com

Joseph "Joe" Damon
Of Counsel
T 615.664.5331
joe.damon@nelsonmullins.com

NELSON MULLINS

GET IN TOUCH

Amanda Witt
Partner
T 404.322.6171
amanda.witt@nelsonmullins.com

Jeffrey M. Kelly
Partner
T 919.329.3852
jeff.kelly@nelsonmullins.com

Jennie Cunningham
Of Counsel
T 212.413.9053
jennie.cunningham@nelsonmullins.com

Adrianne Cleven
Associate
T 919.329.3832
adrianne.cleven@nelsonmullins.com

NELSON MULLINS

GET IN TOUCH

Leslie Green
Of Counsel
T 615.664.5339
leslie.green@nelsonmullins.com

Steven A. Augustino
Partner
T 202.689.2947
steven.augustino@nelsonmullins.com

Michael Nemcik
Senior Associate
T 202.689.2819
michael.nemcik@nelsonmullins.com

Jack Pringle, JD, CIPP/US
Partner
T 803.255.9486
jack.pringle@nelsonmullins.com

NELSON MULLINS

GET IN TOUCH

Stephanie Nakash
Associate
T 615.664.5311
stephanie.nakash@nelsonmullins.com

Kevin Tran
Partner
T 615.664.5322
kevin.tran@nelsonmullins.com