Lowenstein Sandler

Client Alert

Data Privacy, Security, Safety & Risk Management

September 17, 2025

Automated Decision-Making Under the Microscope: CPPA Finalizes New CCPA Rules

By Manali Joglekar CIPP/US, CIPP/E, CIPT, Amy S. Mushahwar, and Tricia Y. Wagner CIPP/US, CISSP, CISA

On July 24, 2025, the California Privacy Protection Agency (CPPA) Board unanimously approved a comprehensive set of final regulations under the California Consumer Privacy Act (CCPA), introducing significant new compliance obligations for businesses related to the use of automated decision-making technology (ADMT). The regulations mark a shift toward operational transparency and consumer control over algorithmic decision-making and are expected to take effect beginning January 1, 2026.

Broad Definition of ADMT

ADMT is defined as "any technology that processes personal information and uses computation to replace human decision making or substantially replace human decision making." If a business relies on the output of a tool without human involvement, the CCPA treats the tool as ADMT. This is a broad definition and may encompass flavors of AI/ML but also automation. The new regulations explicitly include profiling and exclude routine tasks like web hosting, spam filtering, and simple data organization unless these tasks significantly replace human judgment. The regulations apply to ADMT used in making significant decisions about consumers, such as those affecting employment, housing, credit, education, healthcare, or access to essential services. This is in keeping with existing concerns regarding discrimination in the use of ADMT under federal law (e.g. fair housing, equal employment).

Key Compliance Requirements Under the Final ADMT Regulations

- Pre-Use Notice Requirement
  Before collecting or repurposing personal data for use in ADMT, businesses must provide consumers with clear, accessible disclosures outlining the intended purpose and nature of the ADMT. As companies begin to deploy these disclosures, our team will be benchmarking the look and feel of the disclosures within the ADMT technology use.

- Right to Know and Appeal
  Consumers must be informed when ADMT is used to make significant decisions about them and have the right to access meaningful information about how the system operates, including its logic, inputs, and outputs. Additionally, consumers must be given the opportunity to appeal such decisions and request human review.

- Right to Opt-Out
  California consumers now have the right to opt out of certain automated decision-making processes, and businesses must now provide consumers the right to opt-out of ADMT by including a separate opt-out link entitled "Opt-Out of Automated Decision-Making Technology" on their websites. However, this right is subject to several important exceptions outlined in the final regulations, which may limit its applicability depending on the context and nature of the processing. For example, opt-outs are not required where consumers can appeal ADMT decisions to a human reviewer who has authority to overturn the decision.

- Opt-In Consent for Sensitive Data
  Explicit opt-in consent is required when ADMT is used to process sensitive personal information or data related to minors. For example, if a learning platform uses ADMT to analyze a minor's performance and learning style and then makes significant decisions, such as recommending a specific educational track, the provider of the learning platform is required to obtain explicit opt-in consent from the minor or the minor's parent's or legal guardians before using minor's

sensitive personal data for such purposes. Also, if a fintech company uses ADMT to evaluate student loan eligibility based on family financial history and student educational data, and if the system processes sensitive financial information, explicit opt-in consent is required before making credit decisions.

- Human Review Exception
  ADMT systems that incorporate appropriate human oversight may be exempt from certain consumer rights provisions, provided the oversight is substantive and documented. This means the business must designate a human reviewer who must be able to review and analyze the output of the ADMT, know "how to interpret and use the output of the ADMT that made the significant decision being appealed, and … have the authority to change the decision based on their analysis."

- Risk Assessment Requirements
  Prior to deploying ADMT for significant decisions or training such systems, businesses are required to conduct written risk assessments. These assessments must clearly outline the purpose of the ADMT, the categories of data involved, potential risks to consumers, safeguards in place, and the anticipated benefits of the processing.

- Vendor and Recordkeeping Obligations
  Companies must revise vendor agreements to ensure third-party providers comply with ADMT-related requirements. Additionally, businesses are expected to maintain thorough records of completed risk assessments, consumer notices, and responses to consumer requests, demonstrating ongoing compliance with the new regulations.

Next Steps for Businesses

The finalized regulations establish a phased compliance timeline. Businesses that use ADMT for significant decisions must meet the new requirements by January 1, 2027.

Businesses should prepare for compliance with these new requirements by taking the following steps:

- Identify ADMT Use Cases
  Conduct a comprehensive inventory of all technologies, whether developed internally or provided by third parties, that may fall under the definition of ADMT. This includes systems used for profiling, eligibility determinations, or other significant decisions affecting consumers.
- Implement Consumer Rights Workflows
  Develop and operationalize processes to support new consumer rights, including pre-use notices, opt-out mechanisms, and appeals. There may be use cases, such as indirect lending, where your company does not have control over the user flow; in such instances, you should communicate with suppliers to ensure they are aware of the new law and are planning for it. Ensure these workflows are integrated into existing privacy and customer service operations, including websites and apps.

- Review and Update Contracts and Policies
  Amend vendor agreements to reflect ADMT-related obligations and ensure third-party providers support compliance. Update internal policies and train relevant teams on the new requirements and procedures.

- Establish Risk Assessment Protocols
  Create a structured framework for conducting risk assessments prior to deploying ADMT. These assessments should align with California's regulatory standards and be embedded into product development and data governance practices.

For questions concerning these new CCPA regulations or assistance with implementation, please contact our team.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

AMY S. MUSHAHWAR
Partner
Chair, Data, Privacy & Cybersecurity
T: 202.753.3825
amushahwar@lowenstein.com

MANALI JOGLEKAR CIPP/US, CIPP/E, CIPT
Senior Counsel
T: 973.597.2540
mjoglekar@lowenstein.com

TRICIA Y. WAGNER CIPP/US, CISSP, CISA
Counsel
T: 202.753.3658
twagner@lowenstein.com