Procopio

Breaking Down California's New ADMT Regulations

Automated Decisions, Real Consequences

April 30, 2025

Elaine F. Harwell, CIPP/US, CIPM
Partner and Privacy Officer
Elaine.Harwell@Procopio.com
619.906.5780

Overview of Discussion

- High Level: What's changing and why it matters
- Automated Decision-Making Technology (ADMT)
- Risk Assessments (scope, contents)
- Cybersecurity Audits (scope, independence, board oversight)
- Timelines for Compliance
- Action plan
- Q&A

What's Changing: High Level

- Broader ADMT scope tied to decision impact
- New pre-use notice, opt-out, and appeal pathways
- Formal risk assessments for high-risk processing; annual submissions after first filing
- Annual cybersecurity audits for significant-risk processing; independence and board certification
- Status:
  - September 2025, Office of Administrative Law approved the final regulations submitted by the California Privacy Protection Agency (the "Agency")
  - Effective January 1, 2026
  - Most Compliance dates in 2027 and beyond

ADMT: Important Definitions & Scope

- ADMT means any technology that processes PI and uses computation to *replace* human decisionmaking or substantially replace human decisionmaking
- "Substantially replace human decisionmaking" means a business uses the output to make a decision without human involvement.
- ADMT:
  - Includes AI/ML (predictive, generative, recognition) and rule-based engines when driving outcomes
  - Includes profiling
  - Excludes pure backend tools (hosting, storage, firewalls, etc.) unless used to make/replace decisions

ADMT: Important Definitions & Scope (Cont'd)

- Key Point: If a business uses ADMT to make a significant decision concerning a consumer it must comply with the ADMT regulations.
- Significant decision means a 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:
  - Significant decision does not include advertising to a consumer
  - Terms are further defined in CCPA Regs section 7001(ddd)

ADMT: Compliance Checklist

- Prepare a compliant Pre-use Notice
- Provide the ability to opt-out of the use of ADMT to make a significant decision concerning the consumer (exceptions may apply)
- Provide consumer with information about the use of ADMT to make a significant decision (request to access ADMT)

ADMT: Pre-use Notice & Transparency

- Provide pre-use notice (can be in Notice at Collection) that includes the following:
  - A “plain-language” explanation of how the business plans to use the ADMT, i.e., how the ADMT processes PI to reach outputs used for significant decisions.
  - Describe the right to opt-out, categories of PI, logic/key parameters, types of outputs generated, human involvement
  - Provide link(s) to opt-out mechanism(s) aligned with consumer interaction channel
  - Alternative process for making significant decision for consumers who opt out
- Business is prohibited from retaliating

ADMT: Opt-Out and Option to Appeal

- Exception to opt-out if:
  - There is a method to appeal the decision to a human reviewer who has the authority to overturn the decision
  - Business provides clear description of how to submit an appeal and enable the consumer to provide information to human reviewer in support of appeal
- Separate exceptions exist based on type of automated decision being made, e.g., education, employment
- Opt-outs must:
  - Offer 2+ methods to opt-out; at least one matches primary interaction channel (e.g., online form)
- Maintain records of appeals, rationales, changes, and timelines

ADMT: Triggers, Examples, Exclusions

- Triggers:
  - Employment, credit, housing, healthcare, education, insurance, or similar significant decisions
- Examples:
  - Résumé screening, loan approvals, coverage eligibility, pricing engines that drive outcomes
- Exclusions:
  - Calculators, spreadsheets, databases used only to organize human input; not decision-making

Risk Assessments: When Required?

- Where processing of consumer PI presents a “significant risk” to consumer’s privacy:
  - Selling of sharing PI
  - Processing sensitive PI
  - Using ADMT for significant decisions
  - Training ADMT/AI
- May leverage assessments under other laws if they meet all required elements; otherwise supplement
- Risk assessment is tied to the initiation of high-risk processing – i.e., before the business begins the processing
- Use a gating process before launch and recurring reviews for existing high-risk uses
- Examples of when a business must conduct a risk assessment are included in the regulations (Section 7150 (c))

Risk Assessments: Requirements

- Identify and document in a “risk assessment report”:
  - The purpose for processing the PI (not in generic terms)
  - The categories of PI to be processed, including any sensitive PI
  - Processing description: purpose, benefits, categories of PI, systems, stakeholders
  - Potential harms (bias, exclusion, security)
  - Planned safeguards for implementation & residual risk
- Implement policies, procedures, and training to ensure ADMT works for the purpose and does not unlawfully discriminate
- Ensure proper accountability
- Identify whether the processing will occur following the risk assessment
- Certain information from the risk assessment must be submitted to the Agency and full risk assessments may be required to be submitted to the Agency or state AG
- Additional requirements if business is training ADMT using PI

Risk Assessments: Submission Timelines & Retention

- First submission: within 24 months of effective date covering assessments from effective date to submission
- Thereafter: submit annually with no gaps for assessments conducted during the period
- Maintain regulator-ready extracts and evidence repository
- Business must retain risk assessment (including original and updated version) for as long as processing continues or for five years after the completion of risk assessment, whichever is later

Cybersecurity Audits: When Required?

- Annual audit if processing presents “significant risk” to consumers’ security
- “Significant risk”:
  - Business derived 50 percent or more of its annual revenues from selling or sharing consumers’ PI in the preceding calendar year, OR
  - Business, as of January 1 of the calendar year, had annual gross revenue in excess of $25 million AND, either:
    - Processed the PI Of 250,000 consumers/households in preceding calendar year, OR
    - Processed the sensitive PI of 50,000 or more consumers in preceding calendar year

Cybersecurity Audits: Scope and Independence

- Audit report assesses each component of the cybersecurity program; identifies gaps and status against prior audits
  - Regulations contain detailed requirements regarding what the audit must cover and what the report must contain
- Auditor independence:
  - Objective review
  - Cannot rely primarily on management attestations
- Utilizing a cybersecurity assessment prepared for another purpose is permissible if meets all requirements of regulations on own or supplemented
- Submission of written certification to Agency that cybersecurity audit completed as required
  - Certification must be by a member of executive management who is directly responsible for cybersecurity-audit compliance
- Retain all audit docs for ≥5 years

Cybersecurity Audits: Assessing the Cyber Program

- Role-based access & privileged account controls; MFA; logging & monitoring
- Encryption at rest/in transit; vulnerability management; patch SLAs
- Pen testing/red-team exercises; incident response testing & after-action reviews
- Vendor risk: DDQ/DPAs, data maps, and continuous oversight

Key Dates: Compliance with Regulations

- Effective Date of Regulations: January 1, 2026
- Comply with ADMT Regulations: January 1, 2027
- Risk Assessments:
  - For any ongoing processing activity requiring a risk assessment initiated prior to January 1, 2026, the business must conduct and document an assessment no later than December 31, 2027
  - For risk assessments conducted in 2026 and 2027, a business must submit certain information to the Agency no later than April 1, 2028.
- Cybersecurity Audits: tiered based on revenue of business

Key Dates: Compliance with Regulations

- Cybersecurity Audits: tiered based on revenue of business
  - Annual revenue > $100 million: First audit conducted and certification filed by April 1, 2028 (for FY 2027)
  - Annual revenue $50 – $100 million: First audit conducted and certification filed by April 1, 2029 (for FY 2028)
  - Annual revenue < $50 million: first audit conducted and certification filed by April 1, 2030 (for FY 2029)

Action Items

- Start by conducting inventory of ADMT/high-risk uses
  - Prepare ADMT pre-use notice
  - Prepare and approve templates for opt-out / appeal
  - Prepare risk assessment template
- Establish governance
- Kick off audit readiness and vendor-risk refresh
- Schedule annual submissions/board briefings
- Build documentation hub

Thank you!

Questions?

Elaine F. Harwell, CIPP/US, CIPM
Partner and Privacy Officer
elaine.harwell@procopio.com
619.906.5780

Procopio