New CCPA Obligations: What Businesses Need to Know

Sharing Our Perspectives | Three Pillars of Privacy Governance Under CPRA

The California Privacy Protection Agency (CPPA) – the first dedicated U.S. state privacy regulator – has recently finalized expansive rules under the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA). These new regulations significantly expand compliance requirements for businesses handling personal data in California. They establish three major pillars of privacy governance that businesses should be aware of:

Privacy Review (Risk Assessments)

- Businesses must conduct formal privacy risk assessments (DPIA-style) before initiating high-risk data processing.
- High-risk triggers include selling/sharing personal data, processing sensitive info, using ADMT, and profiling in sensitive contexts.
- Assessments must detail data use, risks vs. benefits, mitigation measures, and identify the submitting senior executive.

Annual reporting to CPPA begins April 2028; all existing high-risk activities that began before or after Jan 1, 2026 must be assessed by Dec 31, 2027.

"Are we ready for rigorous privacy assessments?"	"Do we know where our high-risk data processing lives?"	"What's our plan for certifying compliance under penalty of perjury?"
Risk assessments must be reviewed and updated at least every 3 years or sooner and retained for as long as the processing continues or for 5 years after completing the assessment. This shifts privacy from a legal checkbox to a governance imperative.	Selling/sharing data, sensitive info, and AI training all trigger mandatory assessments. Do we have visibility into these activities across business units?	Starting in 2028, companies must submit annual attestations to regulators. Are internal processes strong enough to support executive sign-off?

Where are you in your assessment journey?

Is privacy ad hoc, with reactive and inconsistent assessments? Controlled, with a documented, repeatable process? Or optimized, where an integrated, automated process drives improvement? And do you have deep insight into your operations? Identifying your stage is the first step to building your roadmap.

Automated Decision-Making Technology (ADMT)

- ADMT rules apply to AI systems making "significant decisions" (e.g., credit, compensation, employment, healthcare).
- Businesses must provide pre-use notices explaining how ADMT works and its impact on consumers.
- Consumers have rights to opt out or appeal decisions for human review. For human review, businesses must offer clear processes.
- Consumers can request explanations of how ADMT made decisions about them.

ADMT rules take effect January 1, 2027.

"Can we explain our AI decisions to consumers in plain language?"	"What's our fallback if a consumer opts out of an automated decision?"	"Are we confident our AI systems don't discriminate?"
CPPA requires transparency into how ADMT works and how it affects individuals. Are models interpretable enough to meet this standard?	What alternative human-driven processes for hiring, lending, or other significant decisions are available. Are operations ready to support that?	Risk assessments must evaluate bias and fairness. Do we have the evidence to validate that our ADMT is fit for purpose?

Do you trust your automated technology decisions?

Trust in automated technology decisions is complex, with significant skepticism due to known issues and errors. Key processes for ADMT validation include data quality checks, fairness and security audits, and validating the entire consumer journey (notice, opt-out, appeal). Companies should validate, document and create a remediation plan.

Audit scope

- Annual independent cybersecurity audits are mandatory for businesses with significant data risk (based on revenue/data volume).
- Audits must assess security controls (e.g., MFA, encryption, incident response) and identify gaps with remediation plans.
- Executives must certify audit completion annually; reports must be retained for 5 years.

First audits due April 2028 (for >$100M revenue); phased deadlines continue through 2030.

"Are we treating cybersecurity audits like SOX compliance?"	"What happens if our audit reveals gaps and we don't fix them?"	"Do we have a board-level view of our cybersecurity posture?"
CPPA mandates annual independent audits with executive certification. Audit findings are not privileged. They can be used in litigation. Are we prepared for that level of scrutiny?	CPPA expects remediation plans with timelines. Unaddressed weaknesses could expose a company to fines, lawsuits, and reputational damage.	With executive attestations and personal liability in play, is your company's leadership looped into audit results and risk decisions?

Is your security posture ready to adapt to an external audit regime?

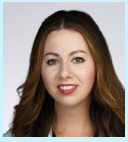
Have you mapped assets, assessed risks, documented and tested controls, trained staff, and established clear, evidence-backed processes that align with the audit's framework (like NIST or SOC 2), demonstrating maturity through consistent monitoring and remediation, with gaps identified and closed? If not, get ready.

Source: Proprietary & Secondary Research; all accessed in January 2026

Contact us

Manoj Thareja
Data Privacy & Protection Leader
KPMG LLP
480-559-1586
mthareja@kpmg.com

Anita Barksdale
Advisory Managing Director
Data Privacy & Protection
KPMG LLP
346-556-7451
anitabarksdale@kpmg.com



Gloria Udrija
Manager, Solution Growth & Strategy
Data Privacy & Protection
KPMG LLP
931-215-8290
gudrija@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**