

California Consumer Privacy Act

Addressing the Final Regulations

An intelligence-led, expert-driven, strategic approach to global cybersecurity & privacy challenges affecting your organization – your people, your operations, and your reputation.

Amendments to the California Consumer Privacy Act (CCPA), finalized in July 2025, introduce new requirements relating to cybersecurity audits, risk assessments, and Automated Decision-Making Technologies (ADMT) for organizations that process personal information of California residents and meet specific thresholds. These updates reinforce the CCPA's continued focus on mitigating risks businesses pose to consumers through their use of personal information. FTI Cybersecurity serves as a trusted partner to help organizations identify privacy and security gaps, address design and governance risks, and advance their path to CCPA compliance.

New Requirements under CCPA's Final Regulations

Cybersecurity Audit

Organizations that meet specific risk criteria are required to conduct annual cybersecurity audits carried out by qualified, independent professionals with expertise in cybersecurity. The regulations also require organizations to implement comprehensive security measures, including strong user authentication, data encryption, access controls, vulnerability testing, network monitoring, regular cybersecurity training, and more. Compliance deadlines for cybersecurity audits will be phased in based on revenue tiers, with the largest companies required to comply by January 1, 2028 and the smallest by January 1, 2030.

Preparing for the audit requirement should start now, as assessing and remediating a cybersecurity program takes meaningful time and planning. Our team of cybersecurity audit professionals are equipped to conduct pre-audit gap assessments now to enable early notification of potential remediation items in advance of the official audits taking place in 2027.

Privacy Risk Assessment

By January 1, 2026, organizations are required to conduct documented risk assessments whenever their data processing activities pose significant risks to consumer

privacy. These activities include selling or sharing personal information, processing sensitive personal information, using ADMT for significant decisions, leveraging consumer information to train ADMT, or using automated tools to draw conclusions about a person's attributes in the context of education, hiring, employment, or independent contracting. Because these requirements are already in effect, organizations without a formal risk assessment process should treat implementation as an immediate priority.

Automated Decision-Making Technology (ADMT)

The final CCPA regulations establish requirements for the use of ADMT, particularly when it is used to "replace or substantially replace human decision-making" in ways that can significantly impact individuals. Organizations that use ADMT as described above must provide clear disclosure to consumers about the use of ADMT, the specific purpose behind its use, and the consumer's rights related to that use. Consumer's rights relating to ADMT include the right to access meaningful information about how decisions involving ADMT were made, the right to request human review and the right to opt-out of ADMT. The ADMT requirements take effect on January 1, 2027.

How FTI Cybersecurity Can Help

FTI Cybersecurity can help organizations navigate the complex requirements of the new CCPA requirements with confidence and efficiency.

Cybersecurity Audit

We have a long history of being engaged as an independent external assessor where we provide unbiased and objective evaluations of an organization's security and privacy programs. We can effectively measure your organization's compliance and security program(s) against CCPA's regulatory requirements and industry accepted standards.

Our experts will help your organization identify areas of vulnerability and provide recommendations in a holistic manner that align to industry standard frameworks for compliance in a risk-based and resource-aware manner. To address this requirement, FTI follows a three phased approach:

Phase 1: Gap Assessment and Remediation

Phase 2: Audit Preparation Activities

Phase 3: Audit Support

Privacy Risk Assessment

We help companies to integrate processes for conducting privacy impact assessments into current operations in order to leverage the workflows relating to their data inventory, third-party onboarding, and/or enterprise risk programs. Having a streamlined operational process is critical to ensuring privacy risk assessments are properly and efficiently conducted.

We help your organization build and sustain a standardized and risk-aligned framework for evaluating privacy risks including designing an operating model, creating assessment templates, and integrating upstream/downstream workflows. Our four phased approach for meeting this requirement includes:

Phase 1: Target Operating Model Development

Phase 2: Trigger Identification & Intake Design

Phase 3: Risk Assessment Integration

Phase 4: Risk Assessment Execution and Reporting

After assessments are completed, remediation actions and related deliverables will be developed, including updating notices, updating or implementing policies and procedures, uplifting security controls, or enhancing consent management.

Automated Decision-Making Technology (ADMT)

Addressing the CCPA ADMT requirements demands more than legal interpretation, it requires operational readiness. Organizations must understand where automated systems influence consumer decisions, evaluate associated privacy risks, and implement governance, transparency, and consumer rights processes.

Our team helps companies translate regulatory obligations into practical, defensible controls by identifying in-scope technologies, embedding oversight frameworks, operationalizing notice and opt-out requirements, and integrating compliance into everyday business workflows.

Why FTI Cybersecurity

Multidisciplinary Expertise

- Intelligence-led, expert-driven, strategic approach to cybersecurity challenges.
- Core team from intelligence agencies, law enforcement, and global private sector institutions

Globally Positioned

- Ability to respond anywhere in the world
- Ability to staff the largest and most complex engagements and investigations
- Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

Integrated & Comprehensive

- Services include crisis communications, e-discovery, forensic investigations, and more
- Seamless integration of FTI Consulting's expertise across service offerings

CASE STUDY**Global Sportswear Company**

Our experts were engaged by a global sportswear company to conduct a comprehensive privacy maturity assessment to evaluate the company's existing privacy controls, policies, procedures, and governance structure against industry best practices and global regulatory requirements, including the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA).

The assessment revealed gaps in the company's ability to effectively manage and document user consent for tracking technologies deployed across its digital properties. Our experts also identified opportunities to develop and enhance the company's Data Subject Access Request (DSAR) program and identified the need for a formal Privacy Impact Assessment (PIA) process. The privacy program maturity assessment provided the global sportswear company with a clear understanding of its current privacy posture and a prioritized roadmap for enhancement. By implementing our recommendations, the company was well positioned to strengthen compliance and reduce regulatory risk.

CASE STUDY**Global Technology Company**

In response to an FTC Consent Order, a global technology company sought a qualified, objective, independent third-party professional to perform initial and biennial assessments of its information security and privacy programs. FTI Cybersecurity was hired as the independent assessor to evaluate the technology company's development of their information security and privacy program and their alignment with the Order.

FTI Cybersecurity leveraged a dedicated team of experts with specific experience designing and assessing information security and privacy programs, especially for global technology companies. This team of experts conducted in-depth discovery efforts to develop and understanding of the operating environment, followed by comprehensive controls design review workshops and then completed operating effectiveness testing based on joint understanding of control operations with the client control owners, with the goal to accurately determine the maturity of its information security and privacy program and its effective adherence to the requirements of the Order.

Jordan Rae Kelly

Senior Managing Director
+1 202 312 9140
jordan.kelly@fticonsulting.com

Elizabeth Kwok

Senior Advisor
+1 415 283 4200
greg.berkin@fticonsulting.com

Ryan Smyth

Managing Director
+1 415 293 4454
ryan.smyth@fticonsulting.com

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm.

FTI Consulting is the leading global expert firm for organizations facing crisis and transformation.

FTI Consulting is dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political and regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.

© 2026 FTI Consulting, Inc. All rights reserved. [fticonsulting.com](https://www.fticonsulting.com)