Capgemini

Take a phased approach to CCPA compliance

A step-by-step guide to preparing for the California Consumer Privacy Act

The California Consumer Protection Privacy Act (CCPA) was passed earlier this year, and it applies to companies that do business in that state or with California residents. Because almost 40 million people live in California, there is a good chance most large businesses in America will have to understand the new CCPA regulation.

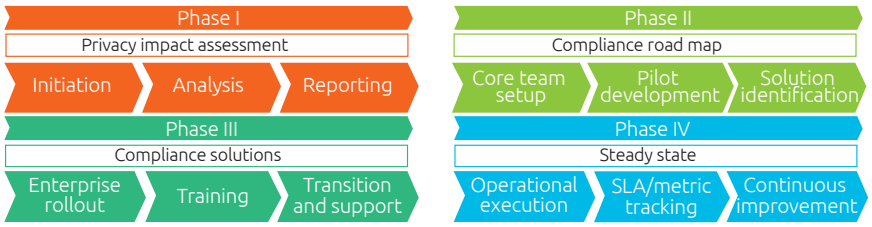
The CCPA actually presents an opportunity to improve brand reputation and customer loyalty. In this entry, we will explain how a phased approach can enable your company's compliance with CCPA and ensure you are ready to reap the advantages it offers.

Our CCPA compliance approach

Technology solutions are integral to achieving CCPA compliance, and the IT department is a key stakeholder. However, data privacy should be seen more from a risk perspective rather than as an IT issue. A CCPA initiative should be overseen by your risk management team or your chief privacy officer (CPO), so compliance is viewed in the context of your company's operational, financial, and reputational risks.

Capgemini recommends a phased approach to CCPA compliance, with four distinct phases.

Phased approach to CCPA compliance



Capgemini recommends a methodical, phased approach to achieving compliance with CCPA

Phase I: Privacy impact assessment

- Identify all relevant stakeholders, both inside and outside your enterprise, and include them in fact-finding interviews and planning workshops
- Perform data discovery to identify and document where personal data exists throughout your organization
- Perform gap analysis to define the delta between as-is state and desired state
- Socialize gap analysis and review with stakeholders
- Plan and prioritize based on risk
- Develop a road map and implementation plan
- Determine a budget for Phase II.

Phase II: Compliance road map

- Establish your core team
- Develop pilots and identify workable solutions for both compliance and organizational needs
- Perform control-gap analysis
- Establish solution requirements
- Finalize responsible, accountable, consulted, and informed (RACI) designations
- Establish workstreams and onboarding teams
- Fine-tune cost and effort estimates
- Execute select pilot projects.

Phase III: Compliance solutions

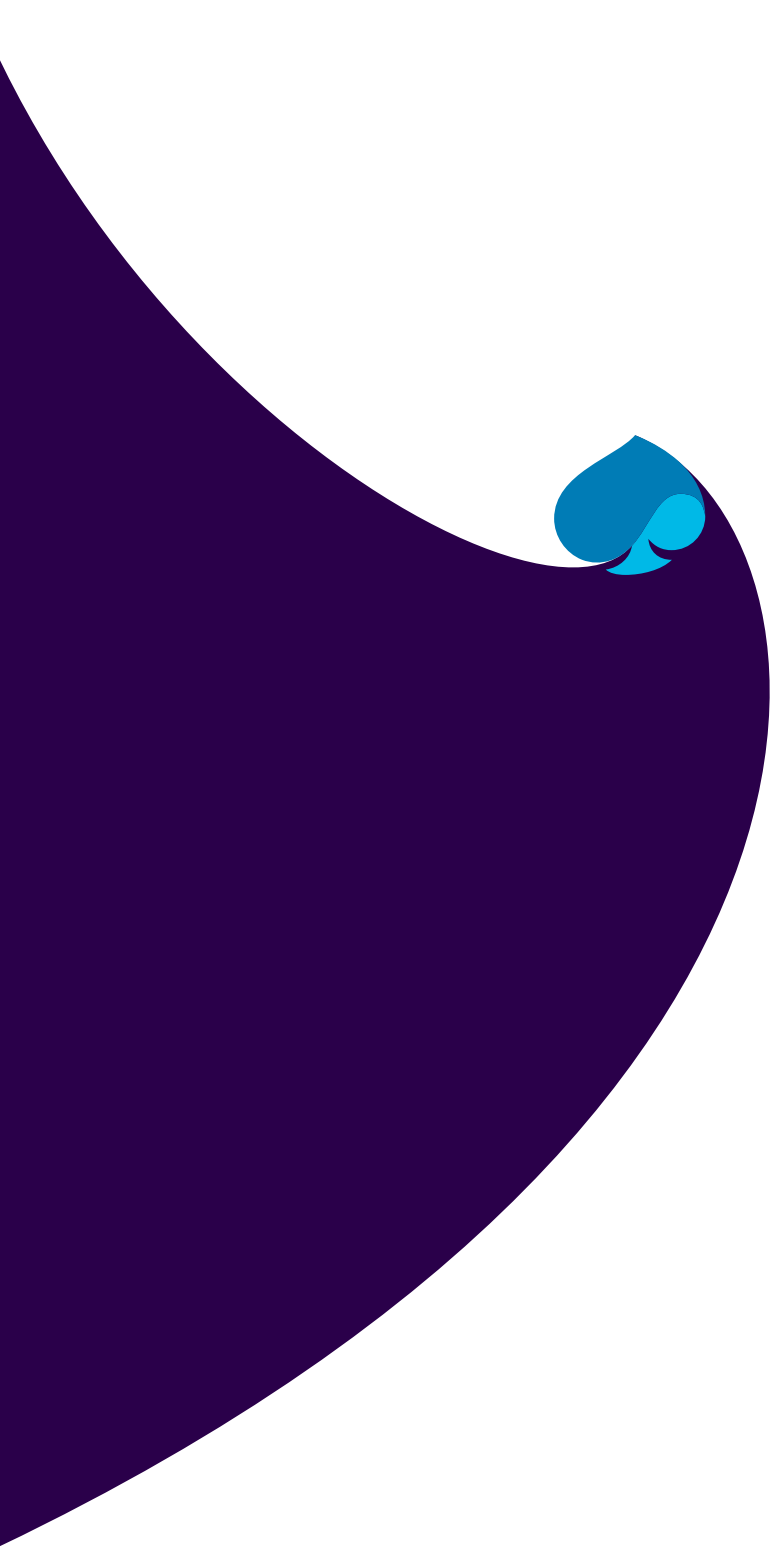
- Create corrective action plans for data security gaps and system vulnerabilities
- Define or revise processes
- Review ongoing initiatives and include remediations
- Update service-level agreements (SLAs) with third parties
- Conduct training to ensure adoption
- Assign employees and processes for transition and support
- Create processes for capturing and reporting metrics
- Formulate pragmatic solutions or services for consent and rights management, including how consent is obtained and re-obtained, and how to execute rights of access and deletion
- Ensure pseudonymizing solutions or services provide anonymized data for marketing and analytics, with role-based access, so you can share data with internal and external stakeholders
- Craft data-protection solutions or services controls to ensure proper protection of both structured and unstructured data. Controls should include access, encryptions, key management, and database access monitoring.

Phase IV: Steady state

- Centralize registry for data privacy regulations
- Define business-as-usual processes for risk management
- Create workflows for remediation activities
- Standardize metrics for measuring outcomes
- Centralize reporting
- Ensure breach-management solutions or services monitor and report on external threats, internal vulnerabilities, personal data repositories and flows, and data-leak prevention
- Create compliance-assurance tools or services to monitor, maintain, update, and continually improve policies, applications, and processes.
- Track metrics and SLAs, identify noncompliant applications and processes, and deliver reports that allow executives to track and manage your company's risk profile.

CCPA compliance doesn't end when your implementation projects are complete. You'll need governance, solutions, and processes to manage your compliance steady state.

Adopting a risk-based phased approach towards CCPA compliance will ultimately support and contribute to your firm's business goals, and a trusted partner can help manage your CCPA lifecycle.



About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 200,000 team members in over 40 countries. The Group reported 2017 global revenues of EUR 12.8 billion (about $14.4 billion USD at 2017 average rate).

Learn more about us at

www.capgemini.com

For more details contact:

Alex Redlich
Privacy Practice Leader, Insights & Data
alex.redlich@capgemini.com

Prasad Lanka
Privacy Engagement Manager, Insights & Data
prasad.lanka@capgemini.com

People matter, results count.