CCPA Project Plan Summary

David Navetta
Partner, Vice Chair
cyber/data/privacy
Cooley LLP
380 Interlocken Cres #900
Broomfield, CO 80021
o: +1 720 566 4153
m: +1 917 306 9314
dnavetta@cooley.com

Cooley

Cooley

cyber/data/privacy

Project Planning Timeline

Timeframe	Actions
Q1 2019	• Get bearings and get started – deadline will come fast • Understand requirements • Monitor amendment activity and AG rulemaking; consider rulemaking participation • Consider CCPA in risk factor disclosures (e.g., in public filings) • Consider CCPA risk/issues in strategic transactions (e.g., M&A, financings) • Identify CCPA compliance resources and kick-off CCPA compliance projects • Develop project plan and milestones
Q2-Q4 2019	• Gap assess, prioritize efforts and execute remediation plan • Build technical capabilities to honor access, deletion, opt out and other rights • Prepare privacy policy and other externally-facing updates for New Year's release
2020	• **January 1, 2020**: CCPA takes effect: class action plaintiffs can sue for statutory damages for personal information data breaches • **July 1, 2020**: Deadline for final regulations from California AG • **July 1, 2020** (or 6 months after final regulations issued by AG, if earlier): AG may bring enforcement action

Cooley

Compliance Gap Assessment and Remediation

1. Set CCPA strategy and plan for success

- Understand business objectives
- Identify relevant legal requirements
- Gather basic information about the business and how it collects, uses and shares personal information
- Design the overall project approach
- Identify and mobilize appropriate stakeholders
- Begin to identify in scope business processes and systems

2. Perform due diligence and gap assessment

- Assess current state of data protection governance
- Gather information about the current collection, use and sharing of personal information
- Gather information about current states of technology and information security
- Perform gap assessment of current practices against CCPA

Plan → Gap Assess

3. Develop prioritized CCPA compliance plan

- Develop prioritized implementation plan to close compliance gaps and control weaknesses
- Identify governance, policy, and technology implementation tracks
- Advise on risk posed by client's desired compliance strategy
- Align with client on next steps for remediating compliance gaps

4. Remediate compliance gaps

- Execute on project plan
- Develop policies, procedures and other artifacts necessary to execute on compliance project plan and to demonstrate compliance in the event of litigation or enforcement action

Prioritize → Remediate

Cooley

Key CCPA Deliverables

Deliverable / Document	CCPA Ref Cal. Civ. Code § 1798	Notes
I. Governance		
a. Compliance Assessment		
i. Gap assessment against CCPA	140(c)(2) 145(c)-(f)	Not explicitly required by CCPA but essential in practice to complete CCPA compliance project. Also, a best governance practice that can help demonstrate accountability to AG or court. Includes determination of whether each covered business has affiliates that will form part of the business for CCPA purposes Includes analysis of whether CCPA exemptions apply
ii. Plan of Action and Milestones (POAM) documenting internal plan for closing compliance gaps		Not explicitly required by CCPA but essential in practice to complete CCPA compliance project. Also a best governance practice that can help demonstrate accountability to AG or court.
b. Data map / inventory of personal information processing activities	130(a) 140(i)	Not explicitly required by CCPA but essential in practice to inform accurate disclosures in privacy policies and in response to consumer information requests
c. Train consumer-facing employees to recognize and triage CCPA opt out requests	135(a)(3)	There are a number of vendors that provide online CCPA training services.
II. External privacy interfaces		
a. Privacy policies		
i. Website/product privacy notice	130(a) 135 140(i) 100(b)	Address CCPA requirements for both the content and presentation of privacy policies
ii. Website/product terms of service		Limited review for consistency with privacy notice/CCPA requirements
iii. Employee/workforce-facing privacy notice	130(a) 135 140(i) 100(b)	Address CCPA requirements for both the content and presentation of privacy policies
iv. M&A notices	140(t)(2)(D	Determine whether any privacy notices to consumers of acquired company are required
v. Notice of intent to re-sell personal information (if applicable)	115(d)	Required only if personal information bought from another party is re-sold

Deliverable / Document	CCPA Ref Cal. Civ. Code § 1798	Notes
b. Data Subject Rights (to access, delete, opt out of sale)		
i. Data Subject Rights Procedure	100, 105, 110 130(a), 135(a)(3) 140(y) 145(g)(1) 192	Describes procedure for how to recognize, triage and respond to data subject requests
ii. Data Subject Rights Communication Templates	100, 105, 110 130(a), 135(a)(3) 140(y) 145(g)(1) 192	Templates for use in communication with data subjects regarding data subject requests
III. Nondiscrimination		
a. Analyze whether different price / service level resulting from opt out requests complies with CCPA nondiscrimination requirements	125	Review service provider agreements to ensure they comply with CCPA service provider requirements and appropriately allocate privacy risk
b. Consent for financial incentive program (e.g., Rewards)	125(b)(3)	Review to ensure compliance with CCPA consent requirements.
IV. Contracts		
a. Service providers		Review service provider agreements to ensure they comply with CCPA service provider requirements and appropriately allocate privacy risk
b. Partners		Review partner agreements to ensure they comply with CCPA service provider requirements and appropriately allocate privacy risk
c. Affiliates		Review or implement inter-affiliate agreements to ensure they comply with CCPA service provider requirements and appropriately allocate privacy liability
V. Information security		
a. Written Information Security Program (WISP)		CCPA does not have security requirements but creates a private right of action for data breaches arising from failure to maintain "reasonable security" under California Civil Code 1798.81.5. WISP refers to the policies and procedures typically implemented to comply with "reasonable security" requirements. Not included in Cooley scope but can be added if desired.
VI. Data retention		

Deliverable / Document	CCPA Ref Cal. Civ. Code § 1798	Notes
a. Document Retention Policy	5(1)(e)	Review existing document retention policy to ensure consistency with CCPA requirements.
VII. Analytics / data strategy		
a. Data Analytics Policy (or other policies/procedures)	140(a) 140(h)	Addresses requirement to implement specific safeguards/processes to use aggregate consumer information, pseudonymous information or de-identified information for analytics, product improvement and other business purposes. Should be aligned with company's broader analytics/data strategy.