The California Consumer Privacy Act:

DWT'S ROADMAP TO COMPLIANCE

1. IDENTIFY AND ASSESS

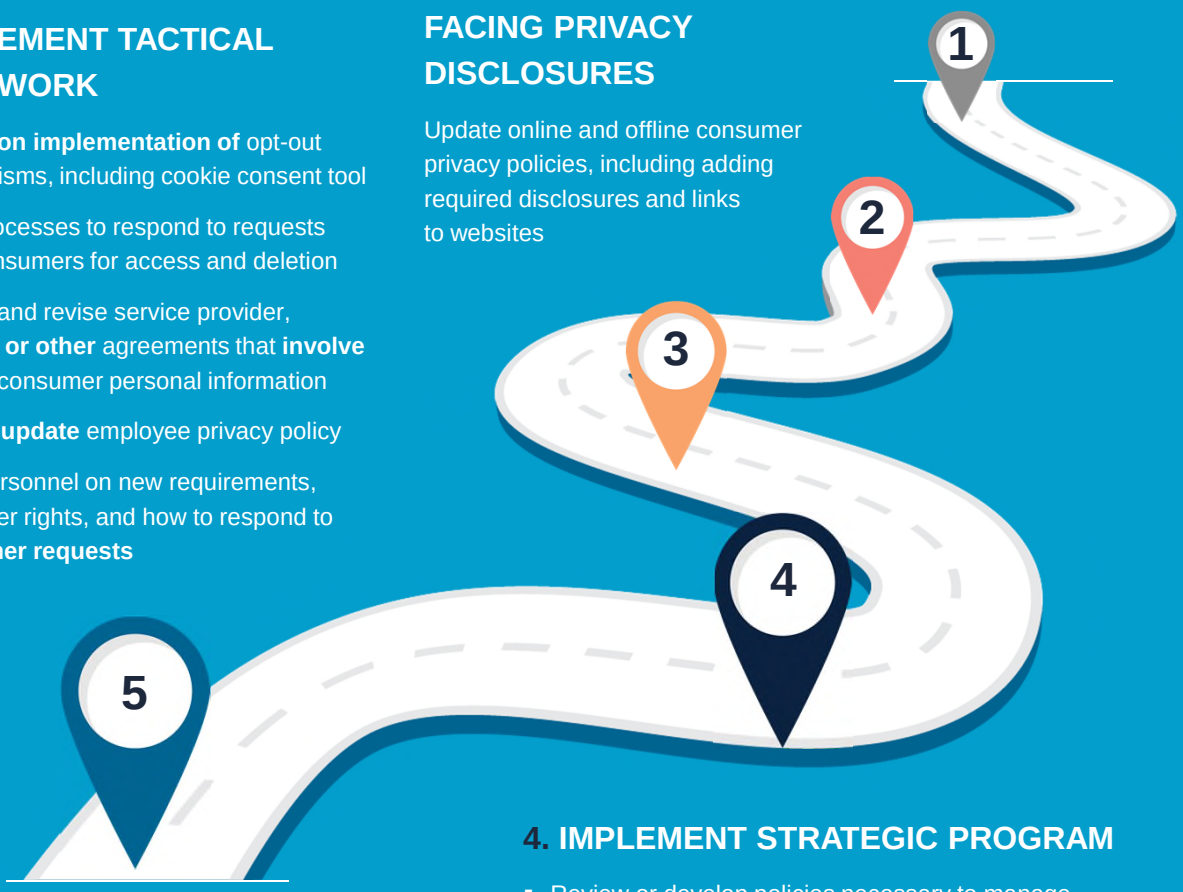
- Conduct holistic review of a business's data processing activities**, as self-reported by the business**
- **Provide template for business to create** inventory of information collection points, systems, and storage locations
- Analyze effects of consumer opt-in / opt-out, access, and deletion rights on operations, including disclosures, processes, and storage

2. UPDATE CUSTOMER-FACING PRIVACY DISCLOSURES

Update online and offline consumer privacy policies, including adding required disclosures and links to websites

3. IMPLEMENT TACTICAL FRAMEWORK

- **Advise on implementation of** opt-out mechanisms, including cookie consent tool
- Draft processes to respond to requests from consumers for access and deletion
- Review and revise service provider, **vendor, or other** agreements that **involve** sharing consumer personal information
- Draft **or update** employee privacy policy
- Train personnel on new requirements, consumer rights, and how to respond to **consumer requests**



4. IMPLEMENT STRATEGIC PROGRAM

- Review or develop policies necessary to manage business records and protect information assets at all stages of data lifecycle, including disposal
- **Update or develop** incident response protocol and security controls

5. ONGOING WORK

- Respond to consumer requests
- Review **and update** privacy and security terms in contracts **on an ongoing basis**
- **Reassess** lessons learned, new risks, and new legal obligations **as needed**

DWT.COM/PRIVSEC

Davis Wright Tremaine LLP

Privacy Essentials

Compliance with modern privacy laws requires a holistic review of a business's data processing activities and may require businesses to rework privacy and information security policies and procedures throughout the information lifecycle. For clients who do not collect and use personal information in complex ways and are just beginning their privacy compliance journeys, DWT offers two options for structuring services:

Option 1: Privacy Essentials Package (fixed fee)

Privacy Essentials is a **risk assessment exercise** intended to identify an organization's operational exposure to privacy laws, particularly the CCPA and GDPR, and **outline steps** required for compliance. **This exercise includes updating an organization's privacy policy.**

Your company will **NOT** be fully compliant after completion of this exercise.

- Instead, it will put you in a position to understand the extent of your compliance obligations and associated costs.
- Full compliance requires a multi-phase approach built into ongoing business processes.

Recommended for: Clients who want to jumpstart compliance while staying within a budget proportionate to their risk.

Option 2: Customized Advice

Where clients prefer to drive project management and creation of work product in-house, DWT can review documents and provide advice on specific questions on an hourly basis.

Services could also include deep-dive risk assessments associated with activities that involve building user profiles, targeted advertising, or loyalty programs.

Recommended for: Clients who have already done work to assess their operations for CCPA impact and who want DWT to focus its efforts on specific areas identified as higher risk.

Deliverables and Pricing

Privacy Essentials	
Process	• Client completes Privacy Practices Self-Assessment Questionnaire • DWT conducts **up to** 3 prescheduled fact-finding interviews (1 hour each) over 1 month • DWT provides Privacy Policy; 1 hour call to review
What You Get	• Compliance checklist and legal action items • Budget for DWT to advise on completion of checklist and deliver additional advice • Data mapping template • Privacy Policy (only one, consumer-facing policy) • CCPA Frequently Asked Questions document
Price	$9,500

Customized Advice	
Process	DWT can provide **services and advice including, but not limited to, the following**: • Initial assessment of potential impact of new privacy laws • Answers to questions arising in the implementation process • Multiple privacy policies (e.g., employee, product-specific, etc.) • Advice on privacy and security terms in specific contracts
What You Get	Specific deliverables **as agreed** at onset of engagement.
Price	Hourly, budget to be provided based on client needs. All engagements will be led by a DWT counsel (billing rate between $595-$680). Where possible, work will be delegated to a DWT associate or paralegal (billing rates between $485-$595).

PRIVACY AND SECURITY – The DWT Team

Rachel Marmor

Counsel
New York
RachelMarmor@dwt.com

With a background as both an external advisor on privacy and security matters and corporate counsel for a global financial institution, Rachel Marmor, CIPP/E, is uniquely poised to counsel clients on a range of legal issues related to data governance and emerging technologies. Rachel prides herself on her ability to create pragmatic business solutions, allowing her clients to maximize the value of their information assets amid ever-changing global legal requirements.

Rachel helps clients assess legal obligations and risks associated with the collection and use of data in their business processes, including privacy, retention requirements, cybersecurity, defensible disposal, and use of electronic data in litigations and investigations. Leveraging her deep expertise in the EU General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA"), Rachel advises clients on the foundational policies and consumer-facing procedures required for effective information management.

Alex Reynolds

Counsel
Washington, D.C.
AlexReynolds@dwt.com

Alex Reynolds, CIPP/US, works collaboratively with clients to identify their privacy and security problems and creates holistic strategies to solve them. When providing advice, Alex seeks to leverage existing resources or discover new ones if the situation requires, recognizes when other DWT experts should be engaged to make efficient use of clients' time, and happily engages in as much or as little project management as clients need. Alex's legal expertise focuses on privacy and security compliance with international law, implementing privacy and security in contracts, and designing data-governance programs to respond to legal obligations.

Emily Bruemmer

Associate
New York
EmilyBruemmer@dwt.com

Emily Bruemmer, CIPP/US and CIPP/E, counsels corporate clients across multiple industries on compliance with intersecting international, federal, and state privacy and data protection laws. Emily works with clients to scope their objectives while navigating compliance challenges in these complex regulatory areas. Her experience with international, federal, and state privacy laws and regulations allows her to assist at all stages of development of a corporate privacy or data protection program, including conducting due diligence, drafting privacy policies and notices, advising clients on how to operationalize best practices in information governance and cybersecurity, and advising clients on cross-border data transfer.

DWT.COM/PRIVSEC

Davis Wright Tremaine LLP