ROPES & GRAY

CHECKLIST

TEN STEPS TO **CCPA COMPLIANCE**

Ropes & Gray is committed to helping you understand how the CCPA impacts your organization and working with you to adapt your policies and procedures to ensure compliance. The following checklist is a useful tool that will help your company prepare and maintain airtight compliance standards under the new data privacy regime.

STEP 1: Determine whether your organization is in scope for the CCPA

- Is your organization a for-profit entity? (Nonprofits are not subject to the CCPA)
- Does it collect personal information about California residents?
- Are you a controller—that is, does your organization determine the purposes and means of processing with respect to the data (i.e., why and how data is used)?
- Are some of your data processing operations exempt from HIPAA, GLBA and certain other federal privacy regimes?
- Is your organization "doing business" in California?
- Does your organization meet any one of the following three thresholds?
  - Revenue over $25 million
  - Annually buys, receives for the business's commercial purposes, sells or shares for commercial purposes—alone or in combination—the personal information of 50,000 or more consumers, households or devices
  - Derives 50 percent or more of its annual revenues from selling consumers' personal information

If you answered yes to all of the above, the CCPA will likely apply to data you collect and use about California residents. Even if not, the CCPA may apply if business partners require compliance by contract or if an affiliate of your organization shares common branding with your organization and satisfies the above criteria.

STEP 2: Establish a governance structure

- To successfully comply with the CCPA, organizations must have in place appropriate compliance structures with established roles and responsibilities.
- As a practical step, organizations may consider appointing a formal privacy lead (or committee) with accountability for CCPA compliance.

STEP 3: Develop and maintain data inventory

- Unlike the GDPR, the CCPA does not expressly require every organization to develop a written record of processing.
- Understanding what data an organization collects and how it is used and disclosed is essential for effective CCPA compliance; if no data map exists, jump-start the process by documenting material flows.
- Organizations must also determine whether personal information is being "sold" as that term is defined by the CCPA.
- As a best practice, organizations should develop and maintain a data inventory documenting what data they collect and store, how it is used, and whether it is disclosed or sold.

STEP 4: Draft externally facing privacy notices

- The CCPA requires organizations to provide information to consumers about the categories of information collected and the purposes for which those categories of information are used.
- Organizations must also update their online privacy notices to include:
  - Details regarding personal information:
    - Categories of personal information collected about consumers
    - Sources from which personal information is collected
    - Purpose for collecting or selling personal information
    - Categories of third parties with whom personal information is shared
  - Express bans on discrimination against the exercise of CCPA rights
  - Sales and disclosures
    - Whether or not the organization sells personal data (must affirmatively state one way or the other)
      - If personal information is sold, describe categories of information sold
    - Whether or not the organization discloses personal information to others for a business purpose
      - If personal information is disclosed, describe the categories of information disclosed
- Consumer rights
  - Describe the following consumer rights:
    - Right to erasure (1798.05)
    - Right to access/portability (1798.110)
    - Right to request additional information about data collection (1798.110)
    - Right to request information about sales or disclosures (1798.115)
    - Right to not be discriminated against if exercising rights (1798.125)
  - List in the online privacy notice one or more methods for submitting consumer rights requests

STEP 5: Develop procedures for responding to and complying with consumer rights requests

- Potential requests include:
  - Right to knowledge, i.e., right to request information specified in sections 1798.110, .115 and .125 of the CCPA
  - Right to access, i.e., right to receive a copy of personal information the organization holds about the consumer
  - Right to portability, i.e., right to have that personal information in a format that is transmittable to another entity, if provided electronically
  - Right to erasure, i.e., right to have personal information deleted, subject to exceptions
  - Right to opt out of sales, i.e., right to restrict the sale of the consumer's personal information
- Develop procedures for verifying the identity of requesters.
- Make available two or more designated methods for submitting requests, including a toll-free number, which may be (and practically should be) the methods listed in the organization's online privacy notice.
- Respond to consumer rights requests within 45 days.
- Nondiscrimination: The organization should establish procedures to avoid discriminating against consumers for exercising the above rights, the so-called right against discrimination, i.e., the right not to be charged a different price or receive different services where exercising the other rights described above, subject to exceptions.

STEP 6: Develop procedures regarding the "sale" of data

- If the organization "sells" data
  - Develop procedures to allow consumers to opt out of such sales
  - Place a clear and conspicuous link on webpages stating "Do Not Sell My Personal Information"
    - Link should enable consumer to opt out of sales
- No obligations if the organization does not "sell" data

STEP 7: Update vendor contracts

- Organizations that wish to fit within an exception to the definition of "sale"—and avoid the "Do Not Sell My Personal formation" obligations—should add contractual terms to their vendor agreements or data processing addenda restricting ongoing uses of data by the vendor.
- Companies will likely wish to add additional terms, such as:
  - Allowing the company to require/request that the vendor delete data in response to consumer rights requests and otherwise assist in responding to consumer rights requests
  - Prohibiting actions that could constitute discrimination against consumers by charging different prices or offering different services
  - Requiring appropriate data security measures

STEP 8: Draft internal privacy policies and procedures to address key issues

- To implement your CCPA compliance program across the organization, publish internal-facing privacy policies governing how personal information is collected, used and disclosed
- The policies and procedures could include, among other things, requirements as to:
  - What information may be disclosed or sold
  - What privacy terms should be included in contracts
  - How to avoid "discriminating" against consumers based on the exercise of their rights
  - How to handle data subject access requests (DSARs)
  - Other fair information practice principles, such as data minimization

STEP 9: Implement appropriate security controls

- Understand what data you are protecting
- Understand the risks you face
- Understand the protections already in place
- Conduct a risk assessment to weigh the benefits and costs of improvements
- Design or maintain controls to respond to the risks identified, taking into account the nature of the personal information your organization collects or stores
- Develop, deploy and routinely test an Incident Response Plan

STEP 10: Develop a process for ongoing monitoring and review of the program

- Integrate CCPA training into employee orientation and annual training
- Plan for personnel and financial resources
- Report on program to senior leadership
- Develop a process for ongoing review and monitoring of the program
- Develop a process to adapt the CCPA to forthcoming similar laws in other states