ROPES & GRAY

CCPA COMPLIANCE **HIGH-LEVEL CHECKLIST**

The California Consumer Privacy Act will enhance privacy rights and consumer protection for residents of California. The following checklist can help companies make sure they comply with the new regulation.

SCOPE

- Is the organization "doing business" in California?
- Does it meet one of 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 not, does the above apply to an affiliate sharing common branding with the organization?
- Does the organization determine the purposes and means of processing with respect to the data?
- Does an exception apply with respect to the data?

Source: 1798.140(c), .145.

COMPLIANCE

- Establish governance structure – someone in charge of privacy/data protection (best practice, not expressly required)
- Develop and maintain data inventory (best practice, not expressly required)
  - Determine whether personal information is being "sold"
- Draft externally-facing privacy notices, including
  - 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
- 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
  - State whether or not the organization discloses personal information to others for a business purposes
    - If personal information is disclosed, describe the categories of information disclosed
- Rights:
  - Describe the following consumer rights
    - Right to erasure (1798.05)
    - Right to access (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 exercise rights (1798.125)
- Designate methods for submitting requests
- Develop procedures for responding to consumer rights requests
  - Rights
    - Right to knowledge, i.e., right to request information specified in sections 1798.110, .115, and .125.
    - Right to access, i.e., right to receive a copy of personal information 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

- Right against discrimination, i.e. right not to be charged a different price or receive different services where exercising the other rights described above, subject to exceptions
  - Develop procedures for verifying the identity of requesters
  - Make available two or more designated methods for submitting requests, including a toll free number (requirement for toll free number likely to be taken out through amendments)

- Develop procedures regarding the "sale" of data
  - If the organization "sells" data
    - Develop procedures to allow consumers to opt out of such sales
    - Place 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

- Update vendor contracts (as necessary)
  - Adding contractual terms restricting ongoing uses of data by the vendor (to fit into exemption for definition of "sale")
  - Adding terms allowing organization to require/request that the vendor delete data in response to consumer rights request

- Draft internally-facing privacy policies to address key issues (best practice, not expressly required), such as:
  - 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
  - Other fair information practice principals such as data minimization

- Implement appropriate security controls (risk assessment first, then design controls to respond to the risks) (not expressly required, but CCPA does create a private right of action arising out of data breaches)
  - Develop, deploy and routinely test an incident response plan (best practice, not expressly required)

- Develop a process for ongoing monitoring and review of the program