Legislation: Final CCPA Regulations Approved

Aug 18, 2020

Authority ★★★★★ **Risk Guidance** ★★★★★ **Control Guidance** ★★★★★

Effective August 14, 2020, businesses must comply with obligations in the AG's Regulations; withdrawn provisions include removal of requirements to obtain explicit consent for new processing purposes, provide offline privacy notices (if businesses substantially interact with consumers offline), ensure opt-out methods are easy for consumers to use and require minimal steps (including use of designs that subvert or impair their opt-out decision), and the option to use the shortform "Do Not Sell My Info" link.

Background Facts:

- the California Office of Administrative Law approved the Attorney General's ("AG") final regulations for the *California Consumer Privacy Act* ("CCPA"):
  - the final regulations were sent for approval in June 2020.

Relevance to Business Activities:

- privacy notice considerations:
  - **notice to consumers:**
    - timely notices provided to consumers shall:
      - use:
        - plain, straightforward language:★
          - avoid technical or legal jargon.★
        - a format that:
          - draws the consumer's attention to the notice;★ and
          - makes the notice readable, including on smaller screens, if applicable.★
      - be:
        - designed and presented in a way that is easy to read and understandable to an average consumer;★
        - available in the languages in which the business in its ordinary course provides:
          - contracts;★
          - disclaimers;★
          - sale announcements;★ and
          - other information to consumers.★
        - reasonably accessible to consumers with disabilities:
          - e.g. online notices can follow generally recognized industry standards, such as the Web Content Accessibility Guidelines.★
        - made readily available where consumers will see it before any PI is collected, e.g.:
          - conspicuous link on a:
            - website homepage;★ or
            - mobile app download page.★
          - prominent signage directing consumers to the web address where the notice can be found.★
      - provide information on how a consumer with a disability may access the notice in an alternative format.★
    - where businesses intend to use consumer PI for purposes that were not previously disclosed, directly notify the consumer of these new uses.★

- where PI is collected:
  - online, notice may be given by providing a link to the section of the business's privacy policy;★ and
  - from mobile devices for purposes consumers would not reasonably expect, provide a just-in-time notice containing a:
    - summary of PI categories being collected;★ and
    - link to the full notice.★
- contents of notices shall include:
  - list of PI categories to be collected:
    - in a manner that provides consumers with meaningful understanding of the information to be collected.★
  - business or commercial use for each PI category;★ and
  - a link:
    - titled "Do Not Sell My Personal Information";★ and
    - to the business's privacy policy.★

○ **indirect collection:**
- notice does not need to be provided where a business does not collect PI directly from consumers:★
  - however, before the PI can be sold, the business must contact the:
    - consumer directly to provide:
      - notice of the sale;★ and
      - information about the right to opt-out.★
    - source of the PI to:
      - confirm that proper notice was provided to the consumer at the point of collection;★ and
      - obtain signed attestations describing how notice was given:★
        - retain for at least two years.★

○ **opt-out notice:**
- this notice must be provided if a business sells consumer PI;★
- businesses that do not operate a website shall establish, document and provide notice using another method;★ and
- opt-out notices are not required if a business:
  - does not, and will not, sell PI collected;★ and
  - states the above in its privacy policy.★

○ **financial incentive notice:**
- notices of financial incentives shall include:
  - a succinct summary of the incentive, price or service difference offered;★
  - description of the material terms of the incentive or price of service difference:
    - including PI categories implicated.★
  - how consumers can opt-out;★
  - notification of the right to withdraw from the incentive;★ and
  - an explanation of why the incentive, price or service difference is permitted under the CCPA, including a:
    - good-faith estimate of the value of PI;★ and
    - description of the method the business used to calculate the value of the consumer's PI.★

○ **privacy policies:**
- policies shall:
  - include a comprehensive description ofpractices for PI collection, use, disclosure, and sale;★
  - be:
    - posted online through a conspicuous link using the word "privacy," on the business's:
      - website homepage;★ or
      - on the download or landing page of a mobile app.★
    - included in any California-specific description of consumer privacy rights.★
  - contain:

        - explanations of:
            - consumer rights; and
            - how consumers can designate an authorized agent to make requests on their behalf.
        - instructions on submitting verifiable consumer requests;
        - the process that will be used to verify requests, including any information that must be provided by the consumer;
        - a contact for questions or concerns; and
        - the date the policy was last updated.
    - not:
        - contain specific pieces of PI about individual consumers; or
        - be personalized for each consumer.
- **minors:**
    - methods reasonably calculated to ensure consent is obtained from parents or guardians include:
        - providing a consent form to be:
            - signed by the parent or guardian under penalty of perjury; and
            - returned to the business by:
                - postal mail;
                - facsimile; or
                - electronic scan.
        - requiring use of a credit, debit card or other online payment system:
            - that provides transaction notification to the primary account holder.
        - having a parent or guardian:
            - call a toll-free telephone number staffed by trained personnel;
            - connect to trained personnel via video-conference; or
            - communicate in person with trained personnel.
        - checking a form of government ID against relevant databases:
            - the ID should be deleted promptly after verification is complete.
    - where affirmative authorization is received by a business, inform the parent or guardian of the:
        - right to opt-out at a later date; and
        - process for doing this on their child's behalf.
    - where there is actual knowledge that minors are between 13 and 16 years:
        - establish, document, and comply with a reasonable process for allowing such minors to opt-in to the sale of their PI; and
        - inform the minor of the:
            - right to opt-out at a later date; and
            - process for doing so.
    - businesses do not have to provide notice of the right to opt-out:
        - if they exclusively target goods or services offers directly to consumers under 16 years and do not sell their PI without affirmative authorization.
- **exceptions:**
    - businesses registered with the AG as a data broker, pursuant to Civil Code 1798.99.80, do not have to provide a collection notice:
        - if registration applications to the AG include links to online notices that explain how opt-out requests can be submitted. ☒ Control
    - until January 1, 2021, when collecting employment-related information, businesses do not have to include the "Do Not Sell My PI" link in notices: ☒ Control
        - a link can be included to paper copies of privacy policies for job applicants, employees, or contractors. ☒ Control
- **removed provisions:**
    - requirements to:
        - obtain explicit consent for new processing purposes; and
        - provide offline notice to consumers if businesses substantially interact with them

offline.

- data governance considerations:
  - **non-discrimination:**
    - financial incentives or differences in service or price:
      - are discriminatory if the business treats the consumer differently because they exercised a CCPA right:
        - e.g. a music streaming site with free and paid premium services where the premium users can opt-out of PI sales:
          - unless the payment amount for premium services is reasonably related to the value of the consumer's data to the business.
      - are permitted if reasonably related to the value of the consumer's data.
    - denial of a consumer request for permitted reasons shall not be considered discriminatory; and
    - estimate the value of a consumer's data by considering:
      - marginal or average value to the business of the sale, collection, or deletion of a typical consumer's data;
      - aggregate value to the business of the sale. collection or deletion of consumers' data, divided by the total number of consumers;
      - revenue generated from:
        - separate tiers, categories, or classes of consumers; or
        - PI sales, collection or retention.
      - expenses related to:
        - PI sale, collection or retention; or
        - offer, provision or imposition of financial incentives or differences in service or price.
      - any other practical and reliable method of calculation used in good-faith.
    - do not offer financial incentives, price or service differences if the business:
      - is unable to calculate a good-faith estimate of the value of the consumer's data; Risk or
      - cannot show that the incentive or difference is reasonably related to the value of the consumer's data. Risk
    - price or service differences that directly result from compliance with federal law shall not be considered discriminatory. Control
  - **prohibitions:**
    - do not:
      - use a consumer's PI for any purpose materially different than those disclosed in the notice at collection; or
      - collect PI categories other than those disclosed in the notice at collection.
  - **training:**
    - all individuals responsible for handling consumer inquiries shall be informed of;
      - all the requirements in the CCPA and these regulations; and
      - how to direct consumers to exercise their rights.

- handling access requests and data governance considerations:
  - **methods for submitting requests:**
    - provide two or more designated methods for submitting requests, including:
      - a toll-free telephone number, at a minimum;
      - an interactive web form accessible through the business's website or mobile app;
      - designated email address:
        - online-only businesses only have to provide an email address for submitting requests.

        - a form submitted:
            - in person; or
            - through the mail.
    - consider the methods the business uses to primarily interact with consumers when determining which methods to provide;
    - where consumer requests are incorrectly submitted or deficient in some manner:
        - treat the request as it had been submitted in the correct manner; or
        - provide the consumer with specific direction on how to remedy the deficiencies.
    - confirm requests within 10 days of receipt, including information about:
        - how the request will be:
            - processed; and
            - verified.
        - when the consumer should expect a response.
    - respond to requests to know or delete PI within 45 days, which begins on the day the request was received:
        - an additional 45 days can be taken to respond to requests, provided the consumer is given notice and an explanation.
- **request verification:**
    - establish, document, and comply with a reasonable method for verifying requestor identity:
        - where feasible:
            - match the identifying information provided with PI maintained by the business; or
            - use a third party identity verification services that complies with these regulations.
        - consider the following factors:
            - PI type, sensitivity, and value of the personal information:
                - sensitive or valuable PI shall warrant a more stringent verification process.
            - risk of harm posed by any unauthorized access or deletion;
            - the likelihood that fraudulent or malicious actors would seek the PI;
            - whether the PI to be provided by the consumer is sufficiently robust to protect against:
                - fraudulent requests; or
                - being spoofed or fabricated.
            - the manner in which the business interacts with the consumer; and
            - available technology for verification.
        - do not require agents to pay a fee for verification.
    - avoid requesting additional information for verification:
        - unless consumer identity cannot be verified from information already maintained by the business:
            - if additional PI is collected, delete it as soon as practicable after processing the request.
    - if the business maintains de-identified consumer information, it is not obligated to:
        - provide or delete this information in response to a consumer request; or
        - re-identify individual data to verify a consumer request.
    - for password-protected accounts:
        - consumer identity can be verified through existing authentication practices; and
        - require consumers to re-authenticate themselves before disclosing or deleting their PI.
    - where fraudulent or malicious activity is suspected, do not comply with requests - unless further verification procedures determine:
        - an authentic request; and
        - the consumer's identity.
    - for consumers that do not have or cannot access a password-protected account:
        - verify their identity to a:
            - reasonable degree of certainty for requests to know PI categories:

        - e.g. matching at least 2 data points provided by the consumer with data maintained.
      - high degree of certainty for requests to know specific pieces of PI or delete PI, e.g.
        - matching at least 3 pieces of PI provided with data maintained; and
        - obtaining a signed declaration, under penalty of perjury, that the requestor is the consumer whose PI is the subject of the request:
          - maintain all signed declarations as part of record-keeping obligations.
    - if there is no reasonable method for verification:
      - state this in all request responses;
      - explain why there is no reasonable method; and
      - evaluate annually whether a method can be established.
- **requests to know:**
  - do not disclose:
    - a consumer's:
      - Social Security number;
      - driver's license number or other government-issued ID number;
      - financial account number;
      - any health insurance or medical ID number;
      - unique biometric data;
      - an account password; or
      - security questions and answers.
    - refer the consumer to the businesses' general practices outlined in the privacy policy - unless the:
      - response would be the same for all consumers; and
      - policy disclosed all required information in response to a request.
  - provide consumers with a meaningful understanding of the:
    - categories of:
      - PI collected, sold or disclosed in the preceding 12 months;
      - PI sources; and
      - third parties.
    - business or commercial purpose for PI collection, use, sale and disclosure.
  - where requests are denied because of a CCPA exception or conflict with federal or state law:
    - provide the requestor with the basis for the denial:
      - unless prohibited to do so by law.
    - disclose other requested information where applicable.
  - if a business maintains a password-protected account with the consumer, a secure self-service portal can be used if it:
    - fully discloses the PI that the consumer is entitled to under the CCPA and these regulations;
    - uses reasonable data security controls; and
    - complies with verification requirements.
  - the 12 month period covered by request shall run from the date the business receives the request:
    - regardless of the time required to verify the request.
  - it is not required to search for PI to respond to requests to know if:
    - PI is:
      - not maintained in a searchable or reasonably accessible format; ☒ Control or
      - maintained solely for legal or compliance purposes. ☒ Control
    - the business:
      - does not sell PI or use it for any commercial purpose; ☒ Control and
      - describes to consumers the categories of records that may contain PI that was not searched. ☒ Control
- **requests to delete:**

- use a 2-step process for online requests to delete where the consumer must:
  - clearly submit the request to delete; and
  - then separately confirm that they want their PI deleted.
- comply with requests by:
  - permanently and completely erasing the PI on existing systems:
    - with the exception of archived or back-up systems.
  - de-identifying the PI; or
  - aggregating the PI.
- deletion of PI stored on archived or backup systems can be delayed until the time of next access or use;
- inform consumers of the:
  - manner in which PI was deleted; and
  - reasons for denying a request:
    - do not use the retained PI for any other purpose.
- the consumer can be presented with the choice to delete select portions of their PI:
  - only if a global option to delete all personal information is also offered, and more prominently presented than the other choices.
- Providers that receive requests from a client's customer shall:
  - explain the basis for a denial; and
  - inform the consumer:
    - that the request should be submitted directly to the client; and
    - of the client's contact information.
- where businesses that deny deletion requests sell the PI:
  - ask the consumer to opt-out of the sale if they have not already made the request.

- **requests to opt-out:**
  - privacy controls shall:
    - clearly communicate or signal that consumers intend to opt-out of PI sales; ☒ Control
    - require consumers to affirmatively select their choice to opt-out; ☒ Control and
    - not be designed with any pre-selected settings. ☒ Risk
  - respect global privacy settings that conflict with consumer's existing business-specific privacy settings or participation in financial incentive programs: ☒ Control
    - notify consumers of the conflict; ☒ Control and
    - allow them to confirm the business-specific setting or program participation. ☒ Control
  - comply with requests as soon as feasibly possible, but no later than 15 business days from receipt: ☒ Control
    - notify third parties the PI has been sold to after the consumer submitted the request, but before the business complied with the request; ☒ Control
    - direct them not to sell the PI; ☒ Control and
    - the consumer does not need to be notified of completion of third party notification. ☒ Control
  - authorized agents can be used to submit requests on a consumer's behalf if they have written permission:
    - deny requests where proof is not submitted.
  - requests do not need to be verified:
    - however, they can be denied if there is a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent:
      - notify the consumer of the reason for denying the request.
- **requests to opt-in:**
  - use a two-step opt-in process where the consumer:
    - clearly requests to opt-in; and
    - separately confirms their choice to opt-in.
  - inform a consumer who has opted-out when a transaction requires the sale of their PI as a

condition of completing the transaction:
    - including instructions on how the consumer can opt-in.★
- **requests to access or delete household information:**
    - for non-password protected accounts with households, do not respond to requests to know specific pieces of PI or delete household PI ☒ Risk - unless:
        - all consumers of the household jointly request to know or delete; ☒ Control and
        - the business:
            - individually verifies all household members; ☒ Control and
            - verifies that each member making the request is currently a member of the household. ☒ Control
    - use existing business practices to process requests relating to password protected accounts; ☒ Control and
    - obtain verifiable parental consent to comply with requests for access or to delete PI of minors under 13 years. ☒ Control
- **authorized agents:**
    - unless the agent has a valid power of attorney, require consumers to:
        - provide authorized agents written permission to submit requests on their behalf;★ and
        - verify their own identity directly with the business.★
    - the obligation to deny requests from agents that do not submit proof of authorization has been removed:
        - instead, a business can deny a request from an authorized agent if they cannot provide the consumer's signed permission demonstrating their authorization.★
- **recordkeeping:**
    - maintain, for at least 24 months, records of:
        - consumer requests made pursuant to the CCPA;★ and
        - how the business responded to the requests.★
    - records may be maintained in ticket or log form if they include the:
        - date of the:
            - request;★ and
            - business's response.★
        - nature of the:
            - request;★ and
            - response.★
        - manner in which the request was made;★ and
        - basis for denial of the request, in whole or in part.★
    - information maintained for record-keeping purposes shall not be:
        - used for any other purpose;★ or
        - shared with any third party:★
            - except as necessary to comply with a legal obligation.★
    - a business:
        - is not required to retain PI solely for the purpose of fulfilling a consumer request; ★ and
        - that annually buys, sells, shares for commercial purposes, or received PI of 10 million or more consumers shall:
            - compile the:
                - number of requests received by type;★ and
                - median number of days taken to substantively respond.★
            - disclose the metrics in their privacy policy by July 1 of each year.★
- **removed provisions:**
    - requirements that opt-out methods:
        - not be designed to subvert or impair consumers' decisions to opt-out has been removed;
        - be easy for consumers to execute; and
        - require minimal steps to allow the consumer to opt out.

- vendor management considerations:
  - **service providers ("Providers"):**
    - Providers cannot:
      - retain, use or disclose PI obtained in the course of providing services ☒ Risk - except to:
        - perform services specified in the written contract with the business that provided the PI; ☒ Control
        - retain and employ another Provider as a subcontractor; ☒ Control
        - use internally to build or improve service quality: ☒ Control
          - unless this use includes:
            - building or modifying household or consumer profiles; ☒ Risk or
            - cleaning or augmenting data acquired from another source. ☒ Risk
        - detect data security incidents; ☒ Control or
        - protect against fraudulent or illegal activity. ☒ Control
      - sell data on behalf of a business when a consumer has opted-out of PI sales. ☒ Risk
    - when Providers receive requests to know or delete, they shall:
      - respond on behalf of the business; ☒ Control or
      - inform the consumer the request cannot be acted on. ☒ Control

- security - administrative safeguards considerations:
  - **consumer requests:**
    - use reasonable security measures when transmitting PI to consumers.★
  - **request verification:**
    - implement reasonable security measures to:
      - detect fraudulent identity verification activity;★ and
      - prevent unauthorized access to, or deletion of, a consumer's PI.★

- understanding enforcement actions considerations:
  - **enforcement:**
    - violation of the Regulations shall:
      - constitute a violation of the CCPA;★ and
      - be subject to the remedies in the CCPA.★

Source Title and Documents:

California AG - Final Text of CCPA Regulations

https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf Final Regulations

https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/addendum-fsor.pdf Addendum to Final Statement of Reasons