



Client Alerts

California Privacy Protection Agency Action Offers Insights on Compliance with Requirements for Handling Consumer Requests

April 01, 2025 | (Time to read: 3 minutes)

By [Daniel E. Venglarik](#) and [Brent Lehman](#)

Businesses subject to the California Consumer Privacy Act (CCPA) should learn from a recent enforcement action against Honda by the California Privacy Protection Agency (CPPA), which settled for \$632,500.

The CCPA applies to any “business,” which is a term of art under the CCPA that refers specifically to a for-profit company that (a) collects personal information of consumers; (b) determines the purposes and means of processing of the personal information; (c) does business in California; and (d) meets one of the three additional criteria: (i) has annual gross revenues greater than \$25 million, (ii) collects or shares personal information from at least 50,000 California residents per year for commercial purposes, or (iii) derives at least 50% of its annual revenue from selling California consumers’ personal information.

Under the CCPA, consumers have the right to request disclosure by a business of what personal information is being collected by that business, for what purpose, and to whom personal information is sold or shared (“Requests to Know”). Consumers also have the right to correct (“Requests to Correct”) or delete (“Requests to Delete”) collected personal information, to opt-out of sale or sharing of personal information (“Requests to Opt-Out”), and to limit the use and disclosure of sensitive personal information (“Requests to Limit”).

In the enforcement action, the agency found that Honda (1) requested excessive information to process certain consumer requests, (2) failed to provide a “symmetrical” opt-out process, (3) imposed unnecessary verification steps for authorized agents, and (4) neglected to execute required contracts with advertising technology partners.

While this enforcement action was based on the CCPA, six other states—Virginia, Colorado, Connecticut, Utah, Texas, and Florida—mandate analogous consumer request mechanisms, with three more states having passed similar laws that will soon go into effect. Businesses should evaluate their data privacy practices to ensure compliance with such consumer request requirements.

Key Takeaways

1. Excessive Verification Requirements for Data Rights Requests

The CPPA found that Honda required consumers to submit more information than necessary to process their CCPA requests. Honda was found to require the same verification information for opt-out requests and requests to limit use as for requests to know, correct, or delete personal information. The CPPA found that this “unlawfully requires Consumers to provide more information than necessary to exercise their . . . rights to opt-out of sale/sharing of their personal information and to limit the use and disclosure of their sensitive personal information.”

2. Asymmetrical Opt-Out Process

Under the CCPA, companies must ensure that opting out of data sales or sharing is as easy as opting in. The CPPA found that Honda’s process required users to take two steps to opt out but only one step to opt back in, violating the “symmetry in choice” rule.



California Privacy Protection Agency Action Offers Insights on Compliance with Requirements for Handling Consumer Requests

3. Unnecessary Consumer Verification for Authorized Agents

The CCPA determined that Honda required consumers to directly confirm authorized agent requests, a step only necessary for the “verifiable” request categories (“Requests to Know,” “Requests to Correct,” and “Requests to Delete”). The agency interpreted its regulations as prohibiting such verification requirements for “Requests to Opt-Out” and “Requests to Limit”.

4. Failure to Execute Required Contracts

The CCPA mandates specific contractual terms for service providers and third parties to whom data is sold. Honda allegedly failed to enter into required agreements with third-party advertising partners that received consumer data through sales or sharing.

What Businesses Should Do to Ensure Compliance

In light of this enforcement action, businesses should proactively assess their data privacy practices and take the following steps:

- **Minimize data collection for opt-out and use limitation requests** – Only collect the information necessary to locate a consumer in company records.
- **Ensure opt-in and opt-out processes are symmetrical** – The number of steps required to opt in should not be fewer than those required to opt out.
- **Avoid unnecessary consumer verification (as appropriate) for agent-submitted requests** – Do not require consumers to confirm an authorized agent’s request to opt out or limit data processing.
- **Review and update contracts with advertising technology partners** – Ensure proper agreements are in place with third-party data recipients and advertising partners.

With enforcement actions in all states increasing, businesses should take proactive steps to align their data privacy practices with applicable requirements to avoid costly fines and reputational risks. For guidance on compliance, contact [Daniel E. Venglarik](#) and [Brent Lehman](#).

Related People

- Brent Lehman
- Daniel E. Venglarik