

# Draft CPRA Regulations Issued by the California Privacy Protection Agency

## The Bottom Line

- The proposed Regulations include many changes and clarifications to aspects of the CPRA, including, but not limited to: the selling or sharing of consumer personal information to third parties; consumer notice and privacy policy requirements; recognition of opt-out preference signals; and required contractual terms with third-party service providers.
- However, this process is far from over. The CPPA will next take comments from the public on the draft Regulations.

The California Privacy Protection Agency (CPPA) released a working draft of regulations to the California Privacy Rights Act (CPRA) late last month (the Regulations). The 66-page document, which is structured as a redlined version of the existing California Consumer Privacy Act (CCPA) regulations, proposes new and revised definitions, extensive new personal information notice and collection requirements, rules for obtaining consumer consent, restraints around sharing or selling personal information to third parties, consumer opt-out request confirmations, and more.

While the issues are too numerous and extensive for a comprehensive list, some highlights are as follows:

## Key Definitions

The Regulations introduce a number of new definitions, including:

- *Disproportionate Effort* – The Regulations provide some clarity to this term, which is referenced on numerous occasions in the CPRA but never defined within the statutory text. The “disproportionate effort” standard requires businesses to prove that the time and/or resources needed to facilitate a consumer request would be significantly higher than the benefit to the consumer.

- *Opt-out Preference Signal* – Also referenced but never defined in the CPRA is the term “opt-out preference signal,” which the proposed Regulations define as “a signal that is sent by a platform, technology, or mechanism, on behalf of the consumer, that communicates the consumer choice to opt-out of the sale and sharing of personal information and that complies with” the Regulations.

## Requirement for Submitting Requests and Obtaining Consumer Consent

Among the new provisions in the proposed Regulations is Section 7004, which details how businesses must design and implement ways for consumers to submit requests and obtain consumer consent to collect, share or sell personal information. Businesses must incorporate the below principles into their methods for allowing consumers to submit requests and for obtaining consumer consent:

- Use easy to understand language;
- Provide symmetry in choice, where the path for consumers wanting to exercise a more privacy-protective option is no longer than the path to exercise a less privacy-protective action;
- Avoid language or interactive elements that are confusing, such as double negatives and toggles or buttons that make the consumer’s choice less clear;
- Avoid manipulative language or choice architecture, including language or wording that makes a consumer feel guilt or shame for a particular privacy choice or bundling consent to subvert the consumer’s choice; and
- Make requests easy to execute, meaning there should be no unnecessary burdens or frictions involved in the CCPA request process.

Under the proposed Regulations, any method that fails to comply with the above requirements may be considered an illegal “dark pattern,” defined in the CPRA as “a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.”

## Opt-out Preference Signals

While the CPRA gave businesses the option of recognizing opt-out preference signals as a valid consumer privacy request, the proposed Regulations would require businesses to

recognize such signals. The Regulations further detail how businesses should process opt-out preference signals to comply with the CPRA. They also exempt businesses from having to post a “Do Not Sell or Share My Personal Information” link if they meet certain criteria regarding opt-out preference signals in a frictionless manner. The Regulations do not provide technical specifications for opt-out preference signals beyond stating that they should be in “a format commonly used and recognized by businesses,” such as an HTTP header field.

### Required Disclosures

Previously titled “Notices to Customers,” Article 2 of the draft Regulations is renamed “Required Disclosures to Consumers,” and includes many robust changes, including:

- Changes to the notice at collection that businesses provide, and in particular, requirements regarding notice at the point of collection when third parties control that collection. The names of any businesses that are allowed to collect personal information from consumers must be identified. Alternatively, any third parties that control that personal information can have their business practices included in the first party’s privacy policy.
- Additional clarification about the CPRA’s “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links, including specific circumstances in which businesses are exempt from having to post them.

As an alternative to posting separate “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links, the Regulations would allow businesses to use a combined “Your Privacy Choices” or “Your California Privacy Choices” link to facilitate consumers’ exercise of both the right to opt out of the sharing/selling of their personal information and the right to limit sharing of their sensitive personal information.

### Opt-out Requests

Businesses that sell or share personal information are required to provide consumers two or more designated methods for submitting requests to opt out of the sale or sharing of their personal information under the draft Regulations. The draft provides several examples of what those methods can be, incorporating the new opt-out preference signal requirements. Notably, the use of a notification or tool involving cookies is not an acceptable method.

### Agency Audits

Importantly, the Regulations would allow the CPPA to “audit a business, service provider, contractor, or person to ensure compliance with any provision of the CCPA.” There are three

instances when an audit may be performed: (1) to investigate a possible violation; (2) if there is a potential “significant risk” to consumers posed by the business’ collection or processing activities; and (3) if the business has a history of noncompliance with the law “or any other privacy protection law.” These audits may be announced or unannounced, and a business’ failure to cooperate with an audit could lead to enforcement action against that business.

While these are draft Regulations, it is imperative that businesses remain aware of the changes and consider planning to ensure compliance before they take effect, though multiple revisions of the Regulations are likely before they are finalized. A CPPA Board hearing is scheduled for June 8, 2022, when more information about the rulemaking process is expected to be revealed.

---

### **For More Information**

Please contact the attorneys listed below or the Davis+Gilbert attorney with whom you have regular contact.

**Gary Kibel****Partner**

212 468 4918

[gkibel@dglaw.com](mailto:gkibel@dglaw.com)**Zachary Klein****Associate**

212 237 1495

[zklein@dglaw.com](mailto:zklein@dglaw.com)