Bloomberg Law

CCPA and CPRA FAQs

Editor's Note: Words in *italics* are terms specifically defined in the statute or regulations. For additional information, consult our **Glossary**. See **California Privacy Reboot Puts Rights in Spotlight**, **California Voters Strike Back With New Privacy Law** and **What to Write When Rewriting a California Privacy Policy** for Bloomberg Law Analysis of the California privacy landscape.

Q What is the CCPA?

A The **California Consumer Privacy Act** (CCPA), signed into law on June 28, 2018, creates an array of *consumer* privacy rights and *business* obligations with regard to the *collection* and *sale* of *personal information*.

Q When did the CCPA take effect?

A The CCPA went into effect Jan. 1, 2020.

Q Where is the CCPA codified?

A The CCPA is codified at **Cal. Civ. Code § 1798.100 et seq**.

Q Are there accompanying regulations?

A Yes, the regulations are found at **11 CCR § 999.300 et seq.** The CCPA authorizes the California Attorney General to adopt regulations pursuant to **Cal. Civ. Code § 1798.185**.

Q What is the CPRA?

A The **California Privacy Rights Act** (CPRA), also known as Proposition 24, is a ballot measure that was approved by California voters on Nov. 3, 2020. It significantly amends and expands the CCPA, and it is sometimes known as "CCPA 2.0."

Q When did the CPRA take effect?

A The CPRA took effect on Dec. 16, 2020, but most of the provisions revising the CCPA won't become "operative" until Jan. 1, 2023.

Q Which provisions of the CPRA are already in effect?

A Principally, the provisions establishing the California Privacy Protection Agency are already in effect. See **Cal. Civ. Code § 1798.199.10** et seq.

CPRA provisions addressing two popular exemptions – the exemption for personal information collected in the employment context (first added to the CCPA in 2019 by AB 25) and the exemption for personal information collected in business-to-business transactions (created by AB 1355) – went into effect Dec. 16, 2020. The CPRA codifies those exemptions in subdivisions (m) and (n) of **Cal. Civ. Code § 1798.145**. Both exemptions, however, expire Jan. 1, 2023, when the rest of the CPRA becomes operative.

Q Does the CPRA replace the CCPA?

A Not exactly. The CPRA is more accurately described as an amendment of the CCPA. The CPRA specifically states that it "amends" existing provisions of Title 1.81.5 of the California Civil Code (currently known as the CCPA) and "adds" new provisions (related to the establishment of the California Privacy Protection Agency). It is unclear, however, whether Title 1.81.5 will continue to be known as the CCPA or will instead be known as the CPRA effective Jan. 1, 2023.

Q Who enforces the CCPA?

A The CCPA vests the California Attorney General with enforcement authority. Although the CPRA grants the California Privacy Protection Agency "full administrative power, authority, and jurisdiction to implement and enforce" the CCPA, the Attorney General still retains enforcement powers. **Cal. Civ. Code § 1798.199.90** provides that the California Privacy Protection Agency "may not limit the authority of the Attorney General to enforce this title."

Q When will enforcement of the CPRA begin?

A Enforcement of the CPRA will not begin until July 1, 2023, and enforcement will apply only to violations occurring on or after that date. It should be noted, however, that the CCPA's provisions remain in effect and enforceable.

Q What is the California Privacy Protection Agency?

A The California Privacy Protection Agency is a new agency, created by the CPRA, which is vested with "full administrative power, authority, and jurisdiction to implement and enforce" the CCPA.

Q When does the California Privacy Protection Agency assume rulemaking authority?

A The CPRA transfers rulemaking authority from the California Attorney General to the California Privacy Protection Agency effective July 1, 2021, with final CPRA regulations due by July 1, 2022.

Q Who is a 'consumer'?

A A *consumer* is a natural person who is a California resident, as defined in the state's tax regulations (**18 CCR § 17014**).

CCPA and CPRA FAQs

Q What rights do consumers have?

A The CCPA creates six specific rights for *consumers*:

1. The **right to know** (request disclosure of) *personal information collected* by the *business* about the *consumer*, from whom it was *collected*, why it was *collected*, and, if *sold*, to whom. The right to know encompasses the **right to access** specific pieces of *personal information*, as well as the **right to data portability**. The CPRA expands the right to know to include *personal information shared* by the *business*.
2. The **right to delete** personal *information collected* from the *consumer*.
3. The **right to opt-out** of the *sale* of *personal information* (if applicable). The CPRA expands the opt-out right to encompass the *sharing* of *personal information*.
4. The **right to opt-in** to the *sale* of *personal information* of *consumers* under the age of 16 (if applicable). The specific reference to the "right to opt in," found in subdivision (c) of Cal. Civ. Code § 1798.120, has been stricken by the CPRA, but the basis for exercising the right has not changed.
5. The **right to non-discriminatory treatment** for exercising any rights.
6. The **right to initiate a private cause of action** for data breaches.

The CPRA creates two additional rights:

7. The **right to correct** inaccurate *personal information*.
8. The **right to limit use and disclosure** of *sensitive personal information*.

Q What is a consumer's 'personal information'?

A The CCPA defines "*personal information*" as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular *consumer* or *household*.

Q What is a consumer's 'sensitive personal information' (SPI)?

A SPI is a subset of *personal information* newly defined in the CPRA. SPI is *personal information* that reveals:

- a *consumer*'s social security, driver's license, state identification card, or passport number;
- a *consumer*'s account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
- a *consumer*'s *precise geolocation*;
- a *consumer*'s racial or ethnic origin, religious or philosophical beliefs, or union membership;
- the contents of a *consumer*'s mail, email and text messages, unless the *business* is the intended recipient of the communication;
- a *consumer*'s genetic data.

Q What constitutes a 'sale' of personal information?

A The CCPA defines a "*sale*" as selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a *consumer*'s *personal information* by the *business* to another *business* or a *third party* for monetary or other valuable consideration. The CPRA does not make substantive changes to the CCPA's basic definition of "*sale*."

Q What does 'sharing' personal information mean?

A The CPRA defines "*sharing*" as renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a *consumer*'s *personal information* by the *business* to a *third party* for *cross-context behavioral advertising*, whether or not for monetary or other valuable consideration, including transactions between a *business* and a *third party* for *cross-context behavioral advertising* for the benefit of a *business* in which no money is exchanged. "Sharing" is a new concept in the CPRA.

Q Who must comply with the law?

A The CCPA imposes obligations on *businesses*, *service providers*, and *third parties*. The CPRA adds a fourth category: *contractors*.

Q How is a 'business' defined?

A The CPRA defines a "*business*" as:

- a for-profit legal entity
- that *collects consumers' personal information* on its own or by others on its behalf
- that alone or jointly with others determines the purposes and means of the *processing*
- that "does business" in California
- and satisfies at least one of the following thresholds:
  1. has annual gross revenues in excess of $25 million
  2. annually buys, receives, *sells*, or *shares* the *personal information* of 50,000 or more *consumers*, *households*, or devices
  3. derives 50% or more of its annual revenues from *selling consumers' personal information*.

The CPRA slightly modifies each of the threshold factors:

- The first threshold – requiring annual gross revenues in excess of $25 million – is amended to clarify that revenues are calculated by looking at the "preceding calendar year."
- The second threshold increases to 100,000 the number of *consumers* or *households* whose *personal information*, alone or in combination, is bought, *sold*, or *shared* annually by the *business*, but "*devices*" are no longer included in the calculation.

CCPA and CPRA FAQs

- The third threshold is amended to include the *sharing*, in addition to the *selling*, of *consumers' personal information*.

The CPRA also adds two new types of *businesses* to its coverage: (1) a joint venture or partnership comprised of "*businesses*" in which each *business* has at least a 40% interest, and (2) any entity that "voluntarily certifies" to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by, the law.

Q What are the principal obligations of a business?

A A *business* must:

- provide notice of *consumer* rights
- honor *consumer* rights
- fulfill disclosure and retention obligations
- facilitate *consumer* requests
- *implement security safeguards*

Q How is 'service provider' defined?

A A "*service provider*" is an entity that receives *personal information* from or on behalf of a *business* and *processes* that *personal information* on behalf of a *business* pursuant to a written contract that prohibits any retention, use, or disclosure of the *personal information* other than as specified in the contract.

Q What are the principal obligations of a service provider?

A A *service provider* must:

- use *personal information* only to perform services on behalf of a *business* as specified in a contract
- comply with the terms of that contract
- *implement security safeguards*

Q How is 'contractor' defined?

A Newly defined in the CPRA, a *contractor* is akin to a *service provider*, inasmuch as it is bound by the terms of a written contract that sets forth certain restrictions and prohibitions on the use of *personal information*. Unlike a *service provider*, however, the *contractor* includes a "certification" that it understands all of those restrictions and prohibitions and that it will comply with them.

Q What are the principal obligations of a contractor?

A A *contractor* must:

- use *personal information* only to perform services on behalf of a *business* as specified in a contract
- comply with the terms of the contract
- implement security safeguards
- not combine *personal information* received from a given *business* with any *personal information* received from others
- notify the *business* regarding its use of subcontractors, and those subcontractors must be contractually bound to the same terms as the *contractors*.

Q How is 'third party' defined?

A The CCPA defines a *third party* as a legal entity who does not meet the characteristics of a *service provider* and who receives *personal information* from the *business*. The CPRA clarifies that a *third party* is not a *service provider* or a *contractor*, nor is it the *business* "with whom the *consumer* intentionally interacts."

Q What are the principal obligations of a third party?

A A *third party* must:

- use *personal information* consistent with promises made at receipt
- provide *consumers* notice of any new or changed practices
- provide *consumers* with explicit notice of any additional *sales* of *personal information* and provide *consumers* with the opportunity to opt out.

Q What are the consequences for non-compliance?

A The CCPA provides for the following options for imposing liability in the event of non-compliance:

- Civil Penalties – In actions by the California Attorney General, *businesses* can face penalties of up to $7,500 per intentional violation or $2,500 per unintentional violation (but there is an opportunity to cure any alleged violation within 30 days after receiving notice of the alleged violation).
- Damages – In actions brought by *consumers* for security breach violations, *consumers* may recover statutory damages not less than $100 and not greater than $750 per *consumer* per incident or actual damages, whichever is greater. In actions for statutory damages, *consumers* must first provide *businesses* with written notice and an opportunity to cure.
- Non-Monetary Relief – In actions brought by *consumers* for security breach violations, *consumers* may seek injunctive or declaratory relief, as well as any other relief the court deems proper.
- *Businesses* may also be subject to an injunction in actions brought by the Attorney General.

The CPRA's amendments reclassify "civil penalties" as "administrative fines," noting that such fines may be assessed against *service providers* and *contractors*, in addition to *businesses*. The CPRA also states that *businesses*, *service providers*, and contractors can face administrative fines of up to $7,500 for violations involving the *personal information* of *consumers* under 16 years of age where the *business*, *service provider*, or *contractor* has actual knowledge that the *consumer* is under 16.

The CPRA also eliminates the 30-day cure period in the context of administrative actions, replacing it with a non-time-specific opportunity to cure at the discretion of the California Privacy Protection Agency. The CPRA also sets forth details regarding investigations and hearings by the Agency.

In the context of the private right of action, the cure period remains, but the CPRA clarifies that the implementation and maintenance of reasonable security procedures and practices following a breach does not constitute a cure with respect to that breach.