



Mar 22, 2021

Categories:

[Publications](#)

[Technology Blog](#)

Authors:

[Monisha Coelho](#)

CCPA vs. CPRA: What Has Changed and How Can Businesses Prepare?

The California Consumer Privacy Act (CCPA) came into effect on January 1, 2020, to regulate the data collection and usage of individual personal information and data breaches in the state. In November 2020, the California Privacy Rights Act (CPRA) was voted into law. The CPRA enhances the protections provided to California residents under the CCPA. It consequently increases the obligations and liabilities of businesses concerning data privacy, data security, and breaches. For example, the CPRA establishes a new category of data subject to regulation, changes what businesses would be subject to the CCPA, eliminates cure periods, and increases penalties for non-compliance. Most of the CPRA's provisions will become effective on January 1, 2023, but applies to data collected starting on January 1, 2022, giving businesses a limited amount of time to come into compliance with the CPRA's provisions.

The CCPA, and notable changes to it by the CPRA, are explained in the Q&A below:

- **What obligations do companies have under the CCPA?**

California residents may ask businesses to disclose what personal information they have about the individual and what they do with that information, delete the individual's personal information, and not sell the individual's personal information.

Individuals also have the right to be notified, before or at the point businesses collect the individual's personal information, of the types of personal information they are collecting and what they may do with that information.

Generally, businesses cannot discriminate against an individual resident for exercising their rights under the CCPA. Businesses cannot make an individual resident waive these rights, and any contract provision that says an individual waives these rights is unenforceable.

The CCPA only grants rights to individuals (not corporations or other business entities) residing in California, even if the person is temporarily outside the state.

- **To what businesses does the CCPA apply?**

The CCPA applies to for-profit businesses that do business in California and meet any of the following:

- Have a gross annual revenue of over \$25 million;
- Buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices; or
- Derive 50% or more of their annual revenue from selling California residents' personal information.
- The CCPA does not apply to nonprofit organizations.

The CPRA increases and decreases the number of businesses to whom the Act applies. It now applies to for-profit businesses that do business in California and meet any of the following:

- Have a gross annual revenue of over \$25 million;
- *Buy, sell or share the personal information of 100,000 or more California residents or households; (the number of households/consumers increased from 50,000 to 100,000; expands coverage to businesses that "share" consumer data; eliminates "devices"); or*
- Derive 50% or more of their annual revenue from selling or sharing California residents' personal information. *(expands coverage to businesses that "share" consumer data)*
- The CCPA does not apply to nonprofit organizations.

- **What is considered "Personal Information" under the CCPA?**

Personal information is data that identifies, relates to, or could reasonably be linked with a resident's household. For example, it could include a person's name, social security number, email address, records of products purchased, internet browsing history, geolocation data, fingerprints, and inferences from other personal information that could create a profile about an individual's

preferences and characteristics.

- **What does the CPRA's new category of "Sensitive Personal Information" include?**

Similar to the Global Data Privacy Regulation (GDPR) enacted by the European Union, the CPRA introduces a new category of data called "Sensitive Personal Information," which includes government identifying information (driver's license, social security numbers); race, religion, ethnicity, sexual orientation, sex life; exact geolocation; biometric and health data; content of nonpublic communications (text messages, email, mail); financial account information (debit/credit card information along with login credentials). These datasets are subject to new disclosure and purpose use limitations. Consumers have new rights to prevent businesses from disclosing this sensitive personal data and to opt-in or opt-out of such data use.

- **What is not considered "Personal Information" under the CCPA?**

Personal information does not include publicly available information from federal, state, or local government records, such as professional licenses and public real estate/property records.

- **What new consumer rights does the CPRA require businesses to provide consumers?**

The CCPA granted California residents certain rights below. The CPRA expanded those consumer rights:

- Right to know what personal information a business has/collects about the consumer. *The CPRA covers information collected beyond the prior 12 months if data is collected after January 1, 2022.*
- Right to opt-out of the sale of the consumer's data to third parties. *The CPRA now includes the Right to Opt-Out of "sharing" of the consumer's data.*
- Right to have the consumers' personal information deleted. *The CPRA requires businesses to notify third parties to whom*

they have sold/shared the consumer's data also to delete the information.

- Right to not be discriminated against by the business for refusing to allow the business to use/sell the consumer's personal information.
- Right to data portability under the CCPA *has been enhanced under the CPRA so consumers can request specific pieces of their data to be ported/transmitted to another entity, to the extent commercially and technically feasible for the business.*

The CPRA grants consumers several new rights, in addition to those above:

- *Right to Restrict and Limit Use and Disclosure of Sensitive Personal Information.*
- *Right to Opt-Out of automated decision-making technology or "profiling."*
- *Right to Opt-Out of Cross-Context Behavioral Advertising.*
- *Right to Request Information about the automated decision-making processing of personal information and its results.*
- *Right to Correction of personal data with businesses if that information is inaccurate.*

- **What Happens If a Business Violates the CCPA?**

Businesses cannot be sued for most CCPA violations. A business can be sued under the CCPA if there is a data breach, and even then, only under limited circumstances. An individual could sue a business if the individual's nonencrypted and nonredacted personal information was stolen in a data breach as a result of the business' failure to maintain reasonable security procedures and practices to protect it.

If this happens, an individual, or many individuals, can sue a business for the amount of monetary damages the individuals actually suffered from the breach or "statutory damages" of up to \$750 per incident. If individuals want to sue the business for statutory damages, they must give the business written notice of which CCPA sections it violated and give the business 30 days to give the

individuals a written statement that it has cured the violations in the notice and that no further violations will occur.

Individuals cannot sue for statutory damages for a CCPA violation if the business is able to cure the violation and provides the individuals with a written statement that it has done so unless the business continues to violate the CCPA contrary to its statement.

The CPRA has eliminated the 30-day cure period that businesses can currently avail of under the CCPA after being notified by the Attorney General's Office of a reported violation. The CPRA also increases the maximum penalties to \$7,500 where the violations involve minors.

For all other violations of the CCPA, only the Attorney General can file an action against businesses. The Attorney General does not represent individual California consumers. Using consumer complaints and other information, the Attorney General may identify patterns of misconduct that may lead to investigations and actions on behalf of the collective legal interests of the people of California.

California residents also have the ability to file a consumer complaint with the Office of the Attorney General if they believe a business has violated the CCPA. The individuals will need to provide the Attorney General's office with details on how the business violated the CCPA, when, and how the violations occurred.

- **For what kinds of data breaches can a business be sued under the CCPA?**

A business can be sued for a data breach under the CCPA only if certain conditions are met. The type of personal information that must have been stolen is the individual's first name (or first initial) and last name in combination with any of the following:

- The individual's social security number,
- The individual's driver's license number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to identify a person's identity,

- The individual's financial account number, credit card number, or debit card number if combined with any required security code, access code, or password that would allow someone access to the individual's account,
- The individual's medical or health insurance information,
- The individual's fingerprint, retina or iris image, or other unique biometric data used to identify a person's identity (but not including photographs unless used or stored for facial recognition purposes)

This personal information must have been stolen in nonencrypted and nonredacted form.

- **What new provisions impact data processing under the CPRA?**

The CPRA requires businesses to implement and comply with data minimization and retention policies and protocols. The CPRA permits the Attorney General's Office to prepare regulations to penalize businesses that do not implement adequate data minimization and retention protocols, even where there is no data breach. The CPRA also requires businesses to undertake cyber audits.

- Purpose Limitation – Businesses cannot use or collect personal consumer data for a purpose that is incompatible with the original purpose without fresh consumer notice.
- Data Minimization – businesses must minimize the collection, use, storing, and sharing of consumer data to what is reasonably necessary for the business and not process the data for incompatible purposes
- Storage Minimization – businesses must disclose how long they retain each category of consumer data and are barred from holding on to individual personal information for longer than is reasonably necessary for each specific purpose of data use.
- Audit Obligations – businesses must carry out mandatory annual cybersecurity audits and risk assessments when their processing of consumer data presents significant risks to consumers' privacy or security.

The [California Department of Justice](#) website is one of the sources used for this alert and serves as a great resource.

Monisha Coelho represents clients – from startups to multinational corporations – in commercial and corporate matters and litigation before state and federal courts. Monisha is a data security and privacy attorney advising companies on CCPA and CPRA compliance, enforcement, risk mitigation, and litigation. She is licensed to practice law in India and advises clients on cross-border US-India business transactions, litigation, and data privacy matters.

DISCLAIMER: The information contained herein is intended for informational purposes only and should not be construed as professional counsel or legal advice. Seek legal counsel for advice with respect to any legal matter. The information in this document may not reflect the most current developments as the subject matter is extremely fluid and may change daily. The content and interpretation of the issues addressed herein are subject to change.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.