

CPRA vs. CCPA vs. GDPR



How the Difference
Impacts Your Data
Privacy Operations





The **California Privacy Rights Act** (CPRA) enhances CCPA. It enforces stricter protection of consumer privacy, similar to the European Union's GDPR, and adds requirements for businesses.

Key Differences Privacy, Security, and IT Teams Need to Know

| GDPR | CCPA | CPRA |
|---|---|--|
| <p>Enforcement</p> | | |
| <p>The European Data Protection Board (EDPB) ensures uniform application of the rules across the EU. Each member state designates a data protection authority (DPA), an independent, public authority responsible for monitoring the application of GDPR and addressing non-compliance.</p> | <p>Enforced by the office of California's Attorney General.</p> | <p>Establishes the California Privacy Protection Agency (CPPA), vested with full administrative power, authority, and jurisdiction to implement and enforce CPRA.</p> <p>CPRA is governed by a five-person board which appoints a Chief Privacy Auditor to conduct audits of businesses.</p> |
| <p>Scope</p> | | |
| <p>Protects individuals in the EU. Applies outside of the EU when a company sells products or services to individuals inside the EU or when EU individuals are targeted or monitored.</p> <p>Applies both to data "controllers" and data "processors," irrespective of size and whether activity is for profit or not. Several obligations apply to "processors," entities that process personal data on behalf of "controllers."</p> <p>Covers "processing" of personal data, defined to include any operation performed on personal data, including collection.</p> | <p>Protects consumers who are residents of California, including households and individuals. Applies to companies that do business in California and:</p> <ul style="list-style-type: none"> • have annual gross revenue in excess of \$25 million • alone or in combination, annually buys, receives for commercial purposes, sells or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices • derives 50% or more of its annual revenues from selling consumers' PI <p>Covers collection, processing, as well as sale of PI.</p> | <p>Changes the definition of "do business." Increases the CCPA threshold for the number of consumers/households to 100,000 and removes devices from the sources of personal information.</p> <p>Applies to businesses that derive 50% or more of their annual revenues from selling or sharing consumers' PI</p> <p>CPRA distinguishes between two types of advertising: "cross-context behavioral advertising" and "non-personalized advertising."</p> <p>Extends the employee and business-to-business exemption from January 1, 2021 to January 1, 2023.</p> |

Opt-in/Opt-out and Restriction of Processing

Requires businesses to prompt consumers to “accept” cookies and other tracking technologies before progressing on a website. Without a consumer’s explicit consent, businesses can’t collect or share their data.

For consent to be valid under GDPR, a consumer must **actively confirm** their consent, such as by ticking an unchecked opt-in box.

Data subjects may request that a controller restrict any type of data processing of personal data if:

1. The accuracy of the personal data is contested
2. The processing is unlawful, but the data subject prefers restriction to erasure
3. The controller no longer needs the personal data for processing, but data are required by the data subject to establish or exercise a legal claim or defense
4. The data subject has objected to processing pending verification of whether the controller can process on other legal grounds.

Requires businesses to have a “Do Not Sell My Personal Information” or “Do Not Sell My Info” link on websites, giving consumers the right to opt out from the selling and/or disclosing of their personal information.

The opt-out only stops the selling of personal information, and it does not impact other uses of their information.

CCPA’s definition of “sale” applies to the exchange for value of all consumer information, including sharing personal data captured by cookies and other tracking technologies with third parties.

During the CCPA revision process, the Attorney General has clarified:

A business’s methods for submitting requests to opt out shall be **easy for consumers to execute** and shall require minimal steps to allow the consumer to opt out. A business shall not utilize a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer’s decision to opt out.

When a business denies a request to delete and the consumer has not already requested to opt out, the business must ask if the consumer would like to opt out of the sale of personal info and include either the contents, of or a link to, the notice of right to opt out.

Businesses must comply with an opt-out request within **15 business days (vs. 45 days for requests to know and delete)**.

Adds a **right to opt out of automated decision-making technology**, including “profiling,” in connection with decisions related to a consumer’s work performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Opt-out right explicitly extends to **sharing** of PI used for cross-context behavioral advertising.

Strengthens opt-in rights for **minors**. Extends the opt-in right to explicitly include the sharing of PI for behavioral advertising purposes. As with the opt-out right, businesses must wait 12 months before asking a minor for consent to sell or share his or her PI after the minor has declined to provide it.

Personal Data/Information

Focuses on personal data, defined as any information relating to an identified or identifiable natural person (data subject), including publicly available data.

Applies to pseudonymization for information that could be attributed to a person by use of additional information.

Addresses information that relates to, describes, is capable of being associated with, or could be reasonably linked, indirectly or directly, with a consumer or household.

During the CCPA revision process, the Attorney General has clarified:

- Information is considered “Personal Information” based on how the information is maintained; if an IP address cannot reasonably link to a particular consumer or household, it is not Personal Information.*
- When a business collects consumers’ Personal Information through a mobile app, businesses may provide a link to the notice on the download page and within the app such as in the app’s settings menu.
- Just-in-time notice is required for apps that a consumer would not reasonably expect would collect Personal Information.
- In responding to a request to know, a business is not required to search for Personal Information if all of the following conditions are met by the business:
 - Does not maintain the Personal Information in a searchable or reasonably accessible format;
 - Maintains the Personal Information solely for legal or compliance purposes;
 - Does not sell the Personal Information and does not use it for any commercial purpose;
 - Describes to the consumer the categories of records that may contain Personal Information that it did not search because it meets the conditions stated above.

Introduces “sensitive personal information” as a new regulated dataset. Sensitive PI includes government identifiers; financial account and login information; precise geo-location; race, ethnicity, religious or philosophical beliefs, or union membership; content of nonpublic communications (mail, email and text messages); genetic data; biometric or health information; and sex life or sexual orientation information.

Requires the following for sensitive PI:

- Disclosure requirements
- Opt-out requirements for use and disclosure
- Opt-in consent standard for use and disclosure
- Purpose limitation requirements

* This clarification was added in CCPA’s first set of modifications then deleted in the second set. Look for a final decision before enforcement begins.

Right to Erasure/Deletion/Correction/Restriction

Deletion right applies to all data concerning a data subject.

Individuals have the right to erasure of their personal data. Controllers/processors must delete a data subject's personal data if:

- Data are no longer necessary in relation to the purposes for which they were collected
- Processing of the data was subject to consent and no other legal ground for processing exists
- Data subject protests and there is no other legal ground for processing
- Data have been unlawfully processed
- Data must be erased for compliance with a legal obligation
- Data may have been collected from a child
- Controllers don't need to erase personal data if it's necessary:
- For exercising the right of freedom of expression and information
- For compliance with an EU or Member State legal obligation
- For reasons of public health and medicine
- For archiving, scientific or historical research, or statistical purposes, subject to minimization (e.g., pseudonymization)

Deletion right applies only to data collected from the consumer (i.e. not data about the consumer collected from third parties).

Consumers have the right to deletion of their PI, **except** when it is necessary to:

- Complete the transaction for which the PI was provided or perform a contract with the consumer
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity and prosecute those
- Debug to identify and repair errors that impair existing intended functionality
- Exercise free speech (of business or another consumer) or other rights.
- Comply with the California Electronic Communications Privacy Act
- Engage in public or peer-reviewed research in the public interest
- Enable internal uses reasonably aligned with the expectations of the consumer based on their relationship with the business
- Comply with a legal obligation
- Use consumer's PI, internally, in a lawful manner that is compatible with the context in which the consumer provided the information

During the CCPA revision process, the Attorney General has clarified:

When a business denies a request to delete and the consumer has not already requested to opt-out, the business must ask if the consumer would like to opt out of the sale of personal info and include either the contents, of or a link to, the notice of right to opt out.

In responding to a request to delete, a business shall inform the consumer whether or not it has complied with the consumer's request.

Modifies right to delete. Businesses are required to notify third parties to delete any consumer PI bought or received, subject to some exceptions.

Adds right to correction. Consumers may request any correction of their PI held by a business if that information is inaccurate.

Adds right to restrict sensitive PI. Consumers may limit the use and disclosure of sensitive PI for certain "secondary" purposes, including prohibiting businesses from disclosing sensitive PI to third parties, subject to certain exemptions.

Right to Access/ Disclosure

Requires businesses inform consumers of their rights at the point of collection.

Data subjects have the right to request access to their personal data.

If the controller has made the personal data public, it must take reasonable steps to inform others that are processing the data that the data subject has requested erasure and must inform the data subject about those steps upon request.

Controllers and processors must know how to identify a request for access. They must provide the personal data undergoing processing. If it has been requested electronically, data must be provided electronically.

Data subject's requests must be complied within one month from receipt of request and can extend two months if they notify the data subject.

Requires businesses to inform consumers **at or before the point of collection as to the categories** of PI to be collected and the purposes for which the PI will be used.

Consumers have the right to request information about what personal information is collected, how it is processed, for what purposes, and with whom it is shared.

Businesses must **disclose within 45 days of receipt** of a verifiable request. Business may exercise one 45-day extension when reasonably necessary if they notify the consumer within the first 45-day period.

Disclosure includes data covered **12 months before request**.

During the CCPA revision process, the Attorney General has clarified:

In responding to a request to know, a business is not required to search for personal information if all the following conditions are met:

- The business does not maintain the personal information in a searchable or reasonably accessible format;
- The business maintains the personal information solely for legal or compliance purposes;
- The business does not sell the personal information and does not use it for any commercial purpose; and
- The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.

A business shall deny a request to know specific pieces of personal information if it cannot verify the identity of the requester pursuant to these regulations.

A business shall establish, document, and comply with a reasonable method, in accordance with the methods set forth in subsection (a)(2), for determining whether the person submitting a request to know or a request to delete the personal information of a child under the age of 13 is the parent or guardian of that child.

Introduces **“access” terminology**, which helps distinguish a request for specific information from a general request for categories of personal information.

Adds right to access information about automated decision-making. Allows consumers to make access requests seeking meaningful information about the logic involved in the decision-making processes and a description of the likely outcome based on that process.

Portability Requirement

Where the request was made by electronic means, and unless otherwise requested by the data subject, the information should be provided in a commonly used electronic form.

In certain circumstances, a data subject has additional rights to:

- receive a copy of their personal data in a structured, commonly used, machine-readable format
- transmit the data to another controller without hindrance from the original controller, including to have the personal data transmitted directly from the first controller to the second controller

The CCPA does not enumerate an explicit right to data portability, in those terms, but if a consumer makes a request, they have the right to receive their information delivered by mail or electronically.

If delivered electronically, information must be portable and in a readily usable format.

Expands right to data portability. Consumers may request that the business transmit specific pieces of PI to another entity, to the extent it is technically feasible for the business to provide the PI in a structured, commonly used and machine-readable format.

Verification

Does not prescribe specific requirements for identity verification.

Rather, it states “the controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers.”

States that a business shall establish, document, and comply with a reasonable method for verifying that the person making a request is the consumer about whom the business has collected information.

Specifies factors for consideration when choosing methods of verification and outlines specific rules for verification of password-protected accounts, non-account holders, and authorized agents.

During the CCPA revision process, the Attorney General has clarified:

- Use of a consumer’s credit card security code was eliminated as a method of verification for non-account holders
- Consumers can’t be required to pay a fee for identity verification
- Businesses must establish, document, and comply with a reasonable method for determining whether a person submitting a request of a child under the age of 13 is the parent or guardian
- Businesses can deny a request to know specific pieces of personal information if they can’t verify the identity of requestor

High-Risk Assessment/DPIA

Requires DPIAs for any processing likely to risk a data subject's rights.

No DPIA required.
Includes a duty to implement and maintain reasonable security procedures and practices appropriate to the information.

Modifications clarify that the duty also applies to service providers and authorized agents.

Calls for businesses which process consumers' personal information that presents significant risk to consumers' privacy or security, to:

(A) **Perform a cybersecurity audit on an annual basis**, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent.

(B) **Submit to the California Privacy Protection Agency** on a regular basis a **risk assessment** with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public.

Limits on Data Collection/Processing/Storage

Data Minimization – limits data collection to only what is required to fulfill a specific purpose. Data collected and processed should not be held or further used unless this is essential for reasons that were clearly stated in advance to support data privacy.

Purpose Limitation – personal data collected for one purpose should not be used for a new, incompatible purpose.

Storage Limitation – personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

N/A

Data Minimization – collection, use, and retention of personal information shall only be as “reasonably necessary and proportionate to achieve the purposes” for which the personal information was collected.

Purpose Limitation – requires businesses to collect, use, retain, and share personal information only as “reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected.”

Storage Limitation – a business shall not collect data “for longer than is reasonably necessary for that disclosed purpose.”

Penalties

National authorities assess fines that must be effective, proportionate, and dissuasive for each case. For especially severe violations, fines can be up to 20 million euros, or up to 4% of the company's total global turnover of the preceding fiscal year, whichever is higher.

Penalties range from \$2,500 for a non-intentional violation to \$7,500 for an intentional violation. Children's personal information is not treated separately, and violations are subject to the same fines as violations involving adults' personal information.

A business is not liable if it cures any noncompliance within 30 days after being notified of alleged noncompliance.

Consumers can bring a private right of action only if there is a breach of non-encrypted and non-redacted personal information.

Increases fines to \$7,500 for each violation of CPRA involving personal information of consumers under the age of 16.

Eliminates the 30-day cure period following notice of alleged non-compliance.

Expands scope of consumers' privacy right of action to include breaches involving email account credentials.

More Changes Heading Your Way with CPRA

Be prepared for ongoing changes to California's privacy laws. In addition to the CCPA modifications made by the AG, California also has a ballot initiative for significant legislative updates to CCPA, known as the California Privacy Rights Act (CPRA) on the docket for November 2020. If CPRA passes, it will provide consumers with more rights and create a privacy agency to issue guidance and regulations.

CPRA would provide compliance guidance prior to its operative date of January 1, 2023—addressing one of businesses' major grievances with CCPA. The effective date for CCPA would be January 1, 2021, ensuring it can provide guidance before CPRA becomes fully operative in 2023, and can enforce the law as soon as it takes effect. Some of CPRA's other significant updates include:

- New protective measures for Sensitive Personal Information (SPI). This new category is similar to GDPR's "special categories of personal data" definition (pertaining to race/ethnicity, religion, sex life, biometrics, or health) and but goes a step further by including a consumer's mail, email, and text messages as well as account log-in, debit card, or credit card number in combination with any password or access credential; and a consumer's precise geo-location.
- For violations of Children's Personal Information, CPRA would triple the administrative enforcement fines. Any business, service provider, contractor, or person that violates the Act's requirements with respect to the collection

or sale of the personal information of minors under the age of 16 (without consent) would be subject to fines of \$7,500 per intentional violation.

- CPRA would double the consumer threshold for businesses subject to the regulations. CCPA applies to businesses that buy or sell or share, for commercial purposes, the personal information of 50,000 or more consumers, households, or devices. Under CPRA, that would be increased to 100,000 consumers. CPRA also removes the need for a "commercial purpose" in buying or selling of personal information and removes "devices" from the list of consumers or households.

Prepare Your Privacy Program for GDPR, CCPA, CPRA, and Whatever Comes Next

If CPRA is approved it would trigger a series of deadlines ultimately culminating in a January 1, 2023 effective date and July 1, 2023 enforcement date.

Meanwhile, if the lessons of GDPR and CCPA inform the future, we can expect more regulations to evolve and more states and countries to develop their own requirements. You'll need to adjust your privacy operations accordingly.

Think of data privacy operations as a continuous program, not a one and done activity. When you have visibility and control over your use of personal data, you can adapt as you need.

Build a flexible privacy program on a solid foundation with WireWheel. [Schedule a live demo and see how it works.](#)

wirewheel

About WireWheel

Founded in 2016 by a team of privacy and technology experts, WireWheel is a leader in the privacy and data protection space. Leveraging the team's deep privacy expertise, WireWheel has developed an easy-to-use platform that enterprises including large financial institutions, telecoms and consumer-facing brands use to manage their privacy programs.

[wirewheel.io](https://www.wirewheel.io)

