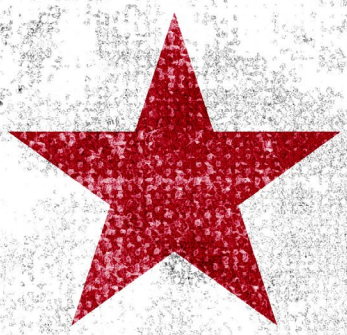
ACA Aponix®



California Privacy Rights Act (CPRA) FAQs

ACA Aponix®
Your trusted partner to help you protect your investments.

Cybersecurity | Privacy | Compliance

ORNIA

What is the CPRA?

The California Privacy Rights Act of 2020 (CPRA) is the latest iteration of data privacy law in the state of California that substantially updates the existing California Consumer Privacy Act (CCPA). It was voted in by California voters on November 3, 2020 as Proposition 24.

The CPRA's enhancement of the CCPA brings California privacy law into closer alignment with the European General Data Protection Regulation (GDPR). Among other additions, the CPRA creates new rights for consumers, adds new governance and transparency obligations for in-scope businesses, introduces a new sensitive data classification, extends data breach liability, and establishes a dedicated agency to interpret and enforce the new law.

When does the CPRA go into effect?

Most of the provisions of the CPRA went into effect on January 1, 2023. Although enforcement of the CPRA was held up in state trial court, a California appeals court ruled on February 9, 2024 that the initial set of regulations outlined in the CPRA can be enforced without delay.

Is the bill final?

The CPRA was voted into law on November 3, 2020 and its effective date was January 1, 2023. Although ballot initiatives are generally difficult to amend without another ballot initiative, the CPRA contains a provision that allows legislative amendments if those amendments are likely to strengthen rather than dilute a consumer's privacy protections. In addition, the new California Privacy Protection Agency (CPPA) will be tasked with interpreting and drafting a final regulation to inform businesses how to comply with key elements of the law.

What are the key changes in the CPRA?

The CPRA provides key changes to the CCPA in the following areas:

New Definitions

The CPRA adds new definitions to California's privacy regulations, including:

- **Third party** – The CPRA defines a third party as any person or legal entity that receives consumer personal information and is not the business, contractor, or service provider. Under the CPRA, contractors and service providers are persons and legal entities with whom the business makes available consumer personal information for purposes defined by the business and pursuant to a written agreement. The CPRA requires businesses that send personal information to third parties, service providers, or contractors to enter into a contract that:
  - Specifies that the personal information is sold or disclosed by the business for limited and specified purposes only
  - Obligates the third party, service provider, or contractor to comply with applicable obligations under the CPRA and to provide the same level of privacy protection as is required by the CPRA
  - Grants the business rights to take reasonable and appropriate steps to help ensure that the third party, service provider, or contractor uses the transferred personal information in a manner consistent with the business's obligations under the CPRA
  - Requires the third party, service provider, or contractor to notify the business if it makes a determination that it can no longer meet its obligations under the CPRA
  - Grants the business the right, upon notice of no longer being able to meet its obligations under the CPRA, to take reasonable and appropriate steps to stop and remediate the unauthorized use of personal information.

For more information, contact us here. **acaglobal.com/aponix**

- **Profiling** – The CPRA defines profiling "any form of automated processing" of personal information to analyze or predict preferences, interests, location, behavior, reliability, movement, etc., unless reasonably expected to perform services or provide requested goods. This new definition will require businesses performing profiling to update notices with detailed descriptions of the logic involved in the decision-making processes and with descriptions of the likely outcomes. Businesses will also need to address new access and opt-out rights related to profiling. The CPRA mandates that the CPPA issue regulations addressing access and opt-out rights where profiling is concerned.

Sensitive Information

The CPRA creates a new "sensitive information" category of applicable privacy information.

The following personal data elements are included:

- Social security numbers
- Driver's license numbers
- Passport numbers
- Financial account information
- Race information
- Ethnicity information
- Religious affiliation information
- Union membership information
- Sex life/orientation information
- Genetic data
- Health information
- Biometric data
- Personal communications
- Geolocation data

This new category of data will create specific rights and obligations that will allow consumers to limit the use and disclosure of their sensitive personal information. Consumers will be able to dictate that a business can only use sensitive personal information for purposes necessary to perform a service or provide goods requested. Authorization will be required to process this data for additional purposes. Further, the CPRA requires that consumers are enabled to limit the sale, sharing and use of their sensitive personal information via the following:

- Companies must post links regarding exercising this right, including a "limit the use of my sensitive personal information" link, and an "opt out of sale or sharing of personal information" link.
- Companies must respect opt-out preferences signaled by the customer with some other platform or technology.

Data Breach Liability

The CCPA and CPRA both build on top of the existing California Breach Notification Law (**California Civ. Code s. 1798.82(f)**). The Breach Notification Law requires "a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person." The CPRA expands the definition of reportable personal information to include breaches resulting in compromises of email addresses in combination with password or security questions/answers, which are now subject to relevant liability.

New Rights

The CPRA adds a number of additional rights to the CCPA. Among the new rights are:

- The right to correct inaccurate personal information
- The right to restrict usage of "sensitive" personal information
- The right to opt out of "sharing" of personal information when personal information is used for the purpose of targeted advertising

For more information, contact us here. **acaglobal.com/aponix**

Data Retention

Per the CPRA, businesses are prohibited from retaining personal information for more time than needed to attain the aims set out in the business' privacy notice. As such, companies will need to ensure they have an understanding of the personal data within their environment, as well as the business requirements for processing that data and the regulatory requirements associated with that data. The regulation does not institute specific retention periods for personal data sets but expects companies to evaluate their personal data and business purposes for processing, to determine retention periods based on the context of their specific processing. The periods should then be documented and communicated to the organization. Once the self-imposed retention periods are reached, the firm should have a process to ensure the data is purged from their environment.

Transparency and Governance

The CPRA adds new transparency and governance requirements, including additional required content in privacy notices, as well as storage limitation and data minimization principles. These include:

- Pre-collection notification - The law modifies the pre-collection notification requirements established in the CCPA to indicate that the notification must be provided at or before collection. The notification must include the categories of sensitive information and the length of time the business retains the information.
- Data minimization – Collection, use, retention, and sharing of personal information must be limited to what is "reasonably necessary" for the specified purpose. For example, if a third party is conducting anti-money laundering (AML) and know your customer (KYC) on a firm's behalf, the firm should evaluate whether there is still a business requirement to collect copies of passports during the subscription process for another business purpose. If not, that information should not be collected and retained in the company's environment.
- Security – Companies must implement "reasonable security procedures and practices" to protect personal information from illegal access, modification, disclosure, or destruction.

"Cross-Context" Advertising

The CPRA enables opting out of "cross-context behavioral advertising," i.e., having information about websites, applications, or services accessed by the consumer shared with others, for use in targeting the consumer with ads from other companies.

New Enforcement Agency

The CPRA creates the California Privacy Protection Agency (CPPA), similar in role to data protection authorities (DPAs) under the GDPR. The CPPA will consist of five members appointed by various governmental shareholders (including the Governor, Attorney General, State Senate, and Speaker of the Assembly). The CPRA will be enforced by the newly established CPPA rather than the California Attorney General's office.

Risk Assessments

The CPPA will be responsible for issuing regulations that require annual audits and regular risk assessments for businesses that conduct high risk processing. Businesses that process consumer data in a way that results in a significant risk to consumers' privacy and security will be required to perform a detailed independent cybersecurity audit on an annual basis. Additionally, businesses processing data in this manner will need to submit regular risk assessments to the CPPA that demonstrate the balances of risks and benefits to the consumers. If risks outweigh the benefits, these firms will be responsible for restricting the processing to appropriately balance these factors.

For more information, contact us here. **acaglobal.com/aponix**

What are the penalities?

The CPRA retains most of the penalties of the CCPA, with the following modifications:

- Cure period – Eliminates the 30-day cure period companies had following alleged non-compliance notification.
- Violations involving minors – Adds a $7,500 penalty for violations involving consumers under 16.

What's next for companies?

As a first step toward CPRA readiness, businesses should conduct a careful review of the CPRA's requirements to identify those elements of the new law that will need to be addressed. The level of effort needed to effectively address these requirements will depend on the relative maturity of the firm's privacy program and whether the privacy program has already addressed the CCPA or other privacy regulations, such as the EU's GDPR. Businesses that have already addressed the CCPA or the GDPR will find themselves in a significantly better position to prepare for the upcoming changes required by the CPRA than those businesses that have yet to implement a privacy program.

In addition to ensuring that your company's privacy program addresses the new CPRA requirements, firms should perform both a cybersecurity assessment to validate that the personal data in their environment is adequately safeguarded as well as a privacy program assessment to validate that their controls and processes have been appropriately implemented and are operating as intended.

Key questions and considerations for determining compliance with the CPRA include:

1. Has the business performed an inventory of its personal data assets? If so, does the inventory include details about sensitive personal data elements and service provider and third-party relationships?
2. Does the business have a records management program that establishes minimum and maximum retention periods? Does this program require the secure destruction or disposal of the personal data once the retention period has been reached?
3. Does the business have a third-party risk management program that requires the firm to conduct due diligence and enter into written agreements with third parties and service providers that receive personal data?
4. Does the business have an individual rights management program? If so, does it address consumers' new rights under the CPRA?
5. Does the business have an incident response plan and breach notification procedure that not only aligns with the current California breach notification regime but also addresses the addition of email addresses in combination with password or security questions/answers to the list of elements in California's breach notification requirements?
6. Has the business evaluated the use of cookies on its website? In particular, has the business assessed whether cookies are being used for targeted advertising and are the appropriate disclosures and opt-out mechanisms in place?

Finally, while the effective date of the CPRA may seem like a long way off, it is important to note that implementing effective privacy programs can take a good amount of time. Further, given that the CPRA has a look back to personal data processed in January 1, 2022, the window to prepare for compliance is significantly shorter. The time to start preparing for the CPRA is now.

For more information, contact us here. **acaglobal.com/aponix**

How we help

ACA's California privacy compliance assistance service is designed to assess your company's readiness to comply with CPRA requirements and to help implement best practices for achieving broader privacy risk and compliance objectives across your enterprise. Our team of experienced consultants can review your company's personal data collection activities, build a data inventory, identify risks and gaps relative to the requirements of CPRA, and assist with building a practical action plan to address deficiencies.

02/2024

ACA Aponix®

For more information, contact us here.

acaglobal.com/aponix