The California Privacy Rights Act

ACA Aponix®

On **January 1, 2023,** the California Privacy Rights Act (CPRA), an amendment to the California Consumer Privacy Act of 2018 (CCPA) goes into effect with a 12-month look back period. The enforcement date is July 1, 2023. The CPRA expands the CCPA's original scope and list of consumer privacy rights regarding the gathering and sale of personal information.

Affected Entities

The CPRA impacts businesses who operate in the state of California and satisfy any of the below criteria:

- Have an annual revenue of over $25 million
- Buy, receive, or sell personal information of 100,000 or more California residents, households, or devices
- Obtain 50% of their annual revenue from selling California resident's information

Service providers, third parties, and now also contractors likewise have legal obligations to adhere to certain regulatory requirements.

Key Terminology

Understanding the Language of CPRA	
Term	**Definition**
Consumer	A natural person who is defined as a "resident" in Section 17014 of Title 18 of the California Code of Regulations, meaning an individual who is not in the state for temporary purposes, *or* resides in the state but is outside temporarily. A consumer does not have to be a customer of a business to be covered by the regulation.
Business	A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that conducts business in the state of California that operates for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal Information.
Service Provider	A person that collects personal information from or on behalf of a business, and processes that personal information on behalf of a business in accordance with a written contract that forbids any retention, usage, or disclosure of the personal information other than as specified in the contract
Contractors	Any person who matches the characteristic of a service provider but demonstrates a certification that they understand contractual restrictions related to the handling of personal information.
Third Party	Any person or entity that is not the business with which a consumer interacts, and is not considered a service provider or contractor, but receives personal information from the business about the consumer.
Personal Information	Information that directly or indirectly identifies, relates to, describes, associates with, or could be linked to a consumer or household, such as (but not limited to): names, aliases, addresses, social security numbers, commercial information, biometric information, network activity, and passport numbers.
Business Purpose	The use of personal information for a business's operational purposes that are reasonably necessary, such as (but not limited to): auditing, securing data, debugging, and providing customer service.

Notable Shifts in Obligations

Changes from CCPA to CPRA	
Change	**Description**
Elimination of the Personal Information Exemption	CPRA rescinds the B2B and employee personal information exemption of the CCPA. Employers with a Californian workforce will need to: • Include employee information in privacy compliance programs • Update compliance practices to accommodate employees in California
Purpose Limitation	A new concept wherein an organization must: • Only process what personal information they need for a specific and legitimate disclosed business purpose
Storage Limitation	A new concept wherein an organization: • Cannot retain personal data once there is no longer a legitimate legal or business need for it
New Consumer Rights	New rights become available to the consumer, including: • The right to correct inaccurate personal information • The right to restrict usage of "sensitive" personal information • The right to opt out of sharing personal information with third parties for cross-context behavioral advertising • The right to opt out of automated decision making
New Sensitive Data Classification	Consumers will have the right to limit the use and disclosure of sensitive information to the specific purpose for which it was originally collected. Sensitive elements include: • Social security numbers • Driver's license numbers • Passport numbers • Account logins • Sex life and orientation information • Genetic and health information • Biometric data • Financial account information • Credit credentials, card numbers, and security code • Geolocation data • Racial or ethnic origin • Religious or philosophical beliefs • Union membership • Personal communications
The California Privacy Protection Agency (CPPA)	CPRA introduced a new agency tasked with: • Establishing rules and procedures to protect consumer privacy rights • Enforcing privacy statues
Vendor Contracting Obligations	CPRA distinguishes between contractors, third parties, and service providers. Contract terms are required with each of these parties New minimum contracting terms include: • Obligating the contracting party to comply with the CPRA • Requiring a contracting party to notify the business if it can no longer comply with CPRA • Granting business rights to ensure that the contracting party is using data appropriately
Required Privacy Notices	The CPRA requires companies to provide consumer notices in the commonly spoken languages of the area that are easy to read and spot, including for those with disabilities. The CPRA requires privacy notices to indicate the following: • Whether information is sold or shared • Length of time businesses intend to retain each category of personal information • Whether sensitive personal information is collected, sold, and/or shared • Which categories of personal information are collected • The use purpose of collected personal information

Penalties

The CPRA retains most of the penalties of the CCPA, with a few modifications.

Pre-existing penalties under the CCPA that will continue under the CPRA include:

- » $2,000 per offense[1] for mistakes
- » $2,500 per offense for negligent mistakes
- » $7,500 per offense for willful offenses

[1] An offense is defined by each record violation. For example, if 500 records are found to be non-compliant with CPRA requirements, the organization would be fined $1 million ($2,000 x 500 records.)

New and/or changes to penalties from the CCPA to CPRA include:

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

Next Steps 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. In addition, organizations 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 optout mechanisms in place?

How ACA Can Help

As the global privacy landscape continues to evolve. ACA Aponix is here to make sense of it. We offer privacy assessments to assess an organization's compliance with emerging or existing privacy regulations, as well as help implement best practices for achieving broader privacy risk and compliance objectives across the enterprise.

Our team of experienced consultants can:

- Review a company's personal data collecting activities to build a data inventory
- Identify risks and gaps relative to the requirements of the privacy frameworks
- Assist with building a practical action plan to address deficiencies

Learn more about our solutions here, or reach out to your trusted cyber advisor.