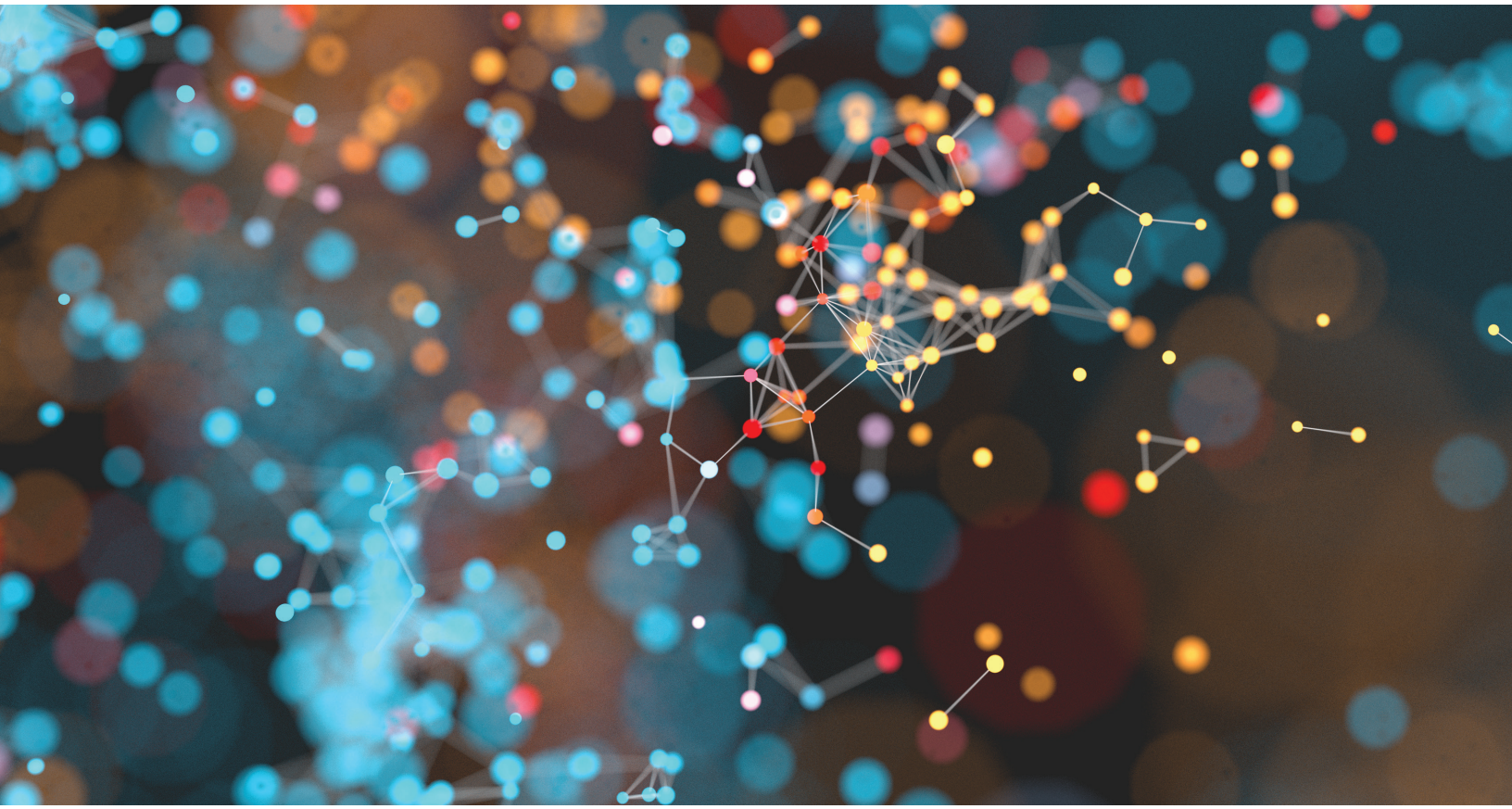
BakerHostetler

A Road Map for CPRA Compliance



The California Privacy Rights Act (CPRA) becomes operative on Jan. 1, 2023. For organizations building a CPRA compliance road map, below is a summary of the requirements under the California Consumer Privacy Act (CCPA), which the CPRA amends, and the key changes under the CPRA. It also includes a checklist of practical compliance actions.

AUTHORS

Jennifer Mitchell
jmitchell@bakerlaw.com

Jeewon Serrato
jserrato@bakerlaw.com

Shruti Bhutani Arora
sbhutaniarora@bakerlaw.com

Marshall Mattera
mmattera@bakerlaw.com

Application and Scope

The CCPA went into effect on Jan. 1, 2020, and enforcement of the law by the California Department of Justice's Office of the Attorney General (OAG) began on July 1, 2020.

The CCPA applies to any for-profit business that "collects" the personal information of California residents, determines the purposes and means of processing the personal

information, does business in California, and meets one or more of the following thresholds:

- Has annual gross revenue that exceeds $25 million.
- Alone or in combination, annually buys, sells, receives and/or shares the personal information of 50,000 or more California consumers, households or devices.
- Derives 50 percent or more of annual revenue from selling personal information.

The CCPA generally does not apply to nonprofit organizations or government agencies, but it may apply to the vendors that provide services to nonprofit organizations or government agencies.

Under the CCPA, "personal information" means 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.

Therefore, "personal information" includes not only identifiers such as names, contact information and government identification but also many other categories of information. These include Internet activity, geolocation, professional or employment-related information, commercial information such as records of personal property, purchase history or preferences, and other data that could be used to link directly or indirectly to a particular consumer or household.

For some organizations, determining the scope of the CCPA could be a straightforward analysis. But for others, it may not be as clear. For example, are IP addresses that are collected by an organization considered personal information under the CCPA? The answer depends on whether the IP address "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."

What's changed under the CPRA

- The CPRA changes the threshold requirements for a covered business. While the $25 million in annual revenue threshold still applies, CPRA changes the threshold number of California residents whose personal information a covered business buys, sells or shares from 50,000 to 100,000.
- The CPRA expands the definition of "business" to include joint ventures or partnerships in which the business has at least a 40 percent interest.
- Under the CPRA, the exemptions related to employee (B2E) and business-to-business (B2B) information expire on Jan. 1, 2023. As noted here, legislators have proposed amendments extending these exemptions, which we will continue to monitor closely. Still, companies are well advised to press forward with compliance efforts assuming that the expirations will occur, to ensure they can comply in time for the CPRA's operation.

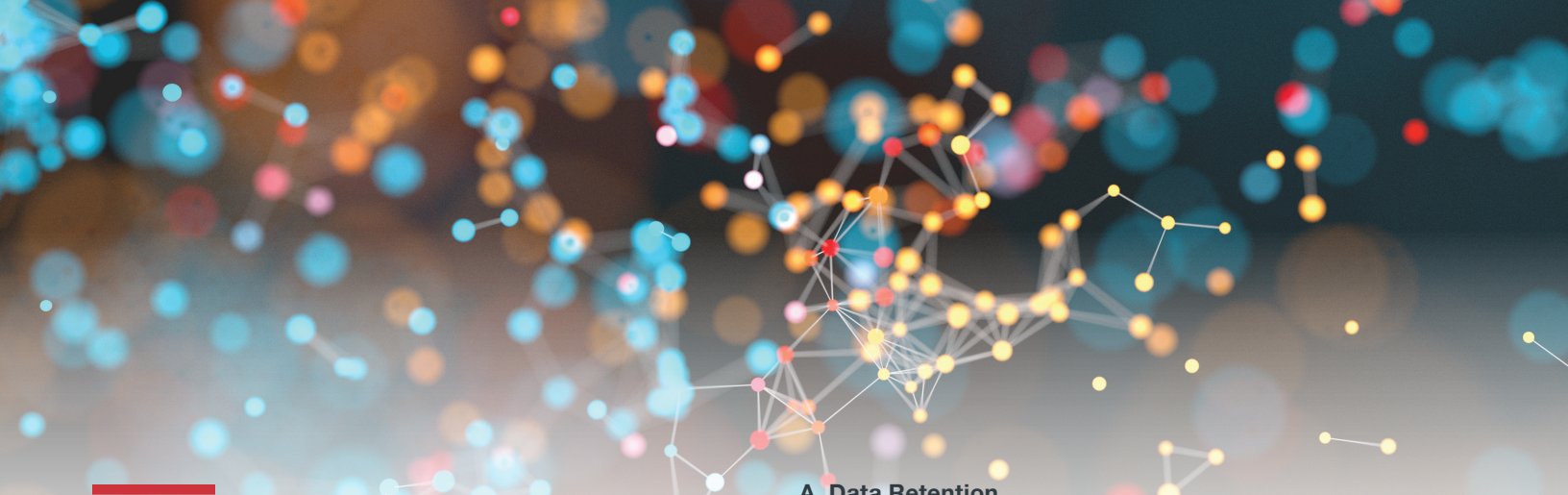
Enforcement Authority

The OAG is responsible for enforcing the CCPA and has authority to impose fines of up to $7,500 per violation. The OAG has published 27 case examples that show that the OAG is actively enforcing the CCPA against a variety of industries, both offline and online.

The CCPA also authorizes private and class action plaintiffs to recover statutory damages of up to $750 per consumer. The private right of action is limited to lawsuits only for certain security incidents, underscoring the importance of sufficient security, but it does not apply to violations of other parts of the CCPA. Companies have various potential defenses and can mitigate risk, for example, through compliant notices and contracts.

What's changed under the CPRA

- In addition to civil enforcement by the OAG and the private right of action, the CPRA provides for both rulemaking and enforcement by the new California Privacy Protection Agency (CPPA). Enforcement is set to begin on July 1, 2023, at which time the CPPA will have the substantial power to impose fines of up to $7,500 per violation.
- The CPRA also eliminates the 30-day period for businesses to cure the alleged noncompliance before being subjected to administrative action. The CPPA will have discretion to allow businesses to cure alleged violations.
- As discussed here, for class actions and other private lawsuits, the CPRA adds a new heading of "Personal Information Security Breaches" that should help confine these actions only to certain security incidents, as originally contemplated for the CCPA.
- The CPRA also expands the scope of actionable personal information to include an email address in combination with a password or security question and answer that would permit access to the email account.
- Under the CPRA, suits for statutory damages that do not comply with the 30-day notice-and-cure period will continue to be improper, and the CPRA adds that reasonable security procedures and practices following a breach will not constitute a cure with respect to that breach.



New and Expanded Data Subject Rights

Under the CCPA, businesses have the obligation to provide notice before personal information is collected and consumers have the right to know, the right to delete, the right to opt out of the sale of personal information and the right to nondiscrimination.

What's changed under the CPRA

A. Opt Out of "Share"

In addition to the right to opt out of "selling," the CPRA provides consumers the right to limit "sharing" of personal information. Under the CPRA, sharing is defined as transferring personal information to a third party for "cross-context behavioral advertising." This type of advertising targets a consumer based on the consumer's personal information obtained from businesses, distinctly branded websites, applications or services that are different from the business with which the consumer intentionally interacts.

B. Limit Use for "Sensitive" Personal Information

The CPRA adds the term "sensitive personal information," not previously defined in the CCPA, which includes information relating to government identification numbers, account access, precise geolocation, race, religion, the contents of written communications, genetic data, biometrics, health and sex life.

The CPRA requires businesses that use or disclose sensitive personal information for certain purposes to provide consumers with notice and a right to limit those uses and disclosures.

C. Right to Correct

Under the CPRA, a consumer will have the right to direct a business to correct incorrect information.

D. Right to Opt Out of Automated Decision-Making

New under the CPRA, businesses will need to provide consumers access and opt-out rights with respect to automated decision-making. Specifically, the CPRA's automated decision-making provisions require businesses to provide a consumer with "meaningful information about the logic" used in automated decision-making.

New Obligations for Businesses

In addition to providing new consumer rights, the CPRA adds new obligations for businesses, service providers and third parties.

A. Data Retention

Under the CPRA, "a business's collection, use, retention, and sharing of a consumer's personal information shall be 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, and not further processed in a manner that is incompatible with those purposes."

B. Cybersecurity Audit and Privacy Risk Assessments

The CPPA is expected to promulgate regulations, requiring businesses engaged in higher-risk processing of personal information to perform a cybersecurity audit on an annual basis and to submit to the CPPA on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and to identify and weigh the benefits resulting from the processing to the business, the consumer, other stakeholders and the public, against the potential risks to the rights of the consumer associated with that processing.

C. Vendor and Third-Party Contracts

The CPRA adds a new "contractor" regulated entity and adds requirements for service providers and third parties. The CPRA adds obligations concerning, for example, coordination between businesses and these third parties regarding consumer request responses, requiring businesses to review and potentially revise written contracts with entities to which personal information is disclosed.

Next Steps

Regulations

The newly created CPPA will be issuing regulations on a number of issue areas, including:

i. Processing activities that present significant risk to consumers' privacy or security.
ii. Cybersecurity audits and risk assessments performed by businesses.
iii. Automated decision-making.
iv. Audits performed by the CPPA.
v. Consumers' right to delete, correct and know their personal information.

vi. Consumers' right to opt out of the selling or sharing of their personal information.
vii. Consumers' right to limit the use and disclosure of their sensitive personal information.
viii. Information to be provided in response to a consumer request to know (specific pieces of information).
ix. Definitions of certain terms covered by the CCPA/CPRA, including "personal information." "sensitive personal information," and "dark patterns."

Compliance Checklist

We recommend considering, at a minimum, the following action steps for your CPRA compliance road map. This checklist is not intended to be exhaustive.

Applicability and Scoping	▪ Is the organization a "Business" under the CPRA? » $25 million annual revenue; ≥50 percent revenue from sales/sharing; or 100,000 consumers/households [devices no longer counted] ▪ What data is in scope?
Data Mapping	▪ Identify collection, use and disclosure of sensitive personal information, and B2E/B2B data ▪ Explore technical solutions and automated tools ▪ Develop maintenance plan for inventory/mapping
Privacy Notices/ Website Updates	▪ Include new disclosures regarding sensitive personal information, new consumer rights and retention periods for personal information ▪ Consider implementation of Do Not Sell/ Share/Limit Processing Website Links and implementation of preference signals, as may be required
Consumer Rights Requests	▪ Develop administrative processes to manage requests and responses, considering new rights and changes to existing rights ▪ Evaluate available technology to track response deadlines and responses for compliance purposes ▪ Develop internal policy and strategy (e.g., When will exceptions apply? How will requests be coordinated?)
Contracts	▪ Consider strategy to update service provider agreements with key clauses ▪ Develop plan to implement written agreements for sharing with third parties who are not service providers ▪ Assess due diligence strategy and process
Data Governance Plan	▪ Take the opportunity to assess data minimization practices ▪ Review data retention policies/practices, and be able to justify retention – e.g., necessity and proportionality
Audits and Risk Assessments	▪ Perform thorough and independent cybersecurity audit on annual basis ▪ Submit risk assessment with respect to processing data to CPPA on a regular basis
Training	▪ Develop training plan for all individuals who handle consumer rights requests so that employees are clear on CPRA rights and their responsibilities ▪ As a best practice, consider developing robust standard operating procedures (SOPs) and other areas of training to demonstrate commitment to privacy compliance

In addition to this checklist, BakerHostetler will continue our Countdown to the CPRA Series and will be providing a series of deep dives into specific CPRA compliance topics, including future blog posts on a CPRA compliance strategy for employee data, the CPRA's impact on data retention and data governance, required updates to privacy policy disclosures, and more.

For more information on and assistance with all things CPRA, please do not hesitate to reach out to the authors and others in BakerHostetler's Digital Assets and Data Management Practice Group.

07.03.22.16.10_p06