The California Privacy Rights Act (CPRA) expands the rights granted to California consumers under the California Consumer Privacy Act (CCPA). The CPRA is an amended and amplified version of the CCPA, which introduces new standards on privacy rights, increased business obligations, and more vigorous enforcement.

The CCPA exceptions for employee personal information and B2B personal information expired on January 1. 2023 - which means that California employers and traditional B2B businesses under the CPRA must take significant steps to achieve compliance. This scenario broadens data protections beyond consumers and extends consumer rights to employees and the management of HR-related and B2B-related personal information.

CPRA Enforcement

Checklist

CPRA Compliance Checklist

The CPRA is in effect and fully enforceable – is your organization compliant? Find out with our comprehensive checklist below.

Map & inventory PI, PII, B2E, and B2B data:

- [ ] Discover, identify, categorize, and index all CA residents, employees, and B2B data
- [ ] Correlate individual information to an identity
- [ ] Assign residency to CA employees and B2B contacts
- [ ] Maintain up-to-date and current documentation of CA employee data flow maps
- [ ] Record, map, and monitor third-party data-sharing flows

Automatically fulfill employee and B2B data rights:

- [ ] Create an intake process for data access rights requests and define workflows
- [ ] Classify and categorize all employee, service provider, and contractor data to include in reports
- [ ] Fulfill DSARs
- [ ] Automate reporting in response to requests
- [ ] Validate data rights (including the right to deletion)

Define breach thresholds & privacy team workflows for breach response:

- [ ] Determine whose data and attributes are impacted by the breach
- [ ] Identify systems and applications that have accessed the breached data source
- [ ] Populate workflows with breach data analysis to facilitate response & notification

Audit & assess privacy risk:

- [ ] Conduct annual internal cybersecurity audits (e.g., size and complexity of the business)
- [ ] Conduct privacy risk assessments (e.g., does the processing involve PI?)
- [ ] Submit risk assessments to the California Privacy Protection Agency (CPPA)

Mitigate risk with retention policies:

- [ ] Define retention policies (e.g., the necessity of consumer data retained)
- [ ] Exercise data minimization practices

Validate & test:

- [ ] Access requests: response, accuracy, & comprehensiveness
- [ ] Data flow maps for assigned business process & associated attributes
- [ ] Data deletion for current state & ongoing data collection
- [ ] Data sharing with third parties, including business purpose & data categories
- [ ] Consent and opt-out operationalization
- [ ] Data retention and minimization
- [ ] Risk Assessment and audits (PIA/DPIA)
- [ ] Security policies for data protection

Update employee notices, privacy statements, service provider agreements, & disclosure notifications:

- [ ] Update privacy statements to reflect changes (e.g., rights, retention, definitions, etc.)
- [ ] If applicable, include new CPRA provisions in employee notices
- [ ] Update existing agreements with service providers, contractors, recruiters, payroll/benefits, IT, cloud, etc
- [ ] Disclose in privacy policies whether employees' personal information was sold or shared, which has been required since January 1, 2023
- [ ] Offer opt-out and alternative mechanisms without discrimination if data is sold or shared

Guidelines for data under the CPRA

‣ The CPRA covers the personal information of employees who are California residents as well as contractors, applicants, and remote workers. The CPRA now defines personal information (social security, phone, shopping history, etc.) to include any data that may be reasonably associated, linked, or related to a CA resident and household.
‣ The CPRA maintains consistent data rights management guidelines but implements stricter requirements for cybersecurity audits, privacy risk assessments, retention policies, and data minimization principles.

Rights of CA employees

‣ **Right to know:**
- The right to disclosure detailing how the employer collects and manages personal data; and the right to copies of "specific pieces of personal information".
- This right could potentially extend to informal communications, HR investigations, and performance.
- Employers must generally comply with such requests within 45 days.

‣ **Right to access:**
- The right to disclosure detailing how the employer collects and manages personal data; and the right to copies of "specific pieces of personal information".

‣ **Right to use and disclosure:**
- The right to request that a business limit its use and disclosure of sensitive personal information.

‣ **Right to delete:**
- The right to request that their data be deleted. This right is not unconditional though. Potential exemptions may apply in reference to personal information necessary for current or past employment or contracted relationships.
- The right to delete was also modified under the CPRA and would require service providers, contractors, and third parties to comply with consumer deletiorequests.

‣ **Right to correct:**
- The right to request that a business correct inaccurate information.

‣ **Right to opt-out:**
- The right to opt-out of having personal information sold or shared.
- The right to opt-out of and request information on the automated decision tools or mechanisms that a business employs. Uses.

‣ **Right to leniency:**
- The right to not be retaliated against for exercising any of their CPRA rights.

How BigID helps with the CPRA

BigID helps organizations manage and adapt to privacy regulation as laws evolve, amend and expand. Organizations can leverage BigID for a holistic data privacy approach, with risk assessments, self-service portal, automated DSAR fulfillment and regulatory reporting - all on a foundation of data discovery covering all data, everywhere.

- **Discover and classify** all CPRA impacted data across the enterprise
- **Map, inventory, and categorize** CPRA data by individual, HR, & B2B data
- **Operationalize** data flow mapping and monitoring privacy risk
- **Leverage** workflows to automate and validate end to end data rights fulfillment
- **Execute** data retention policies at scale
- **Conduct** risk assessments for security purposes
- **Manage and monitor** third-party data sharing

About BigID

BigID enables security, compliance, privacy, & governance for all data, everywhere. BigID is enterprise-ready and built to scale: enabling a data-centric approach to comprehensive cloud data security & DSPM, accelerating compliance, automating privacy, and streamlining governance. Customers deploy BigID to proactively discover, manage, protect, and get more value from their regulated, sensitive, and personal data across their data landscape.

BigID has been recognized for innovation as a 2019 World Economic Forum Technology Pioneer; named to the Forbes Cloud 100; the Inc 5000 for 3 consecutive years; the Deloitte 500 for 3 consective years; Market Leader in Data Security Posture Management (DSPM); Leader in Privacy Management in the Forrester Wave; and an RSA Innovation Sandbox winner.

Find out more at https://bigid.com.

Know Your Data, Control Your Data.

Data Security • Compliance • Privacy • Governance

Reduce risk, accelerate time to insight, and get data visibility and control across all your data - everywhere.

> **Tools like BigID are the future.**
> Organizations should be leveraging these tools to remove the manual processes from data discovery, provide better visibility, and help with prioritization of controls.
>
> Ryan O'Leary
> Future of Trust: Battling Data Discovery Confusion