Data Privacy
Institute

Data Compliance Checklist

Data Privacy Institute (DPI): CPRA 2023 Checklist and Client Questionnaire

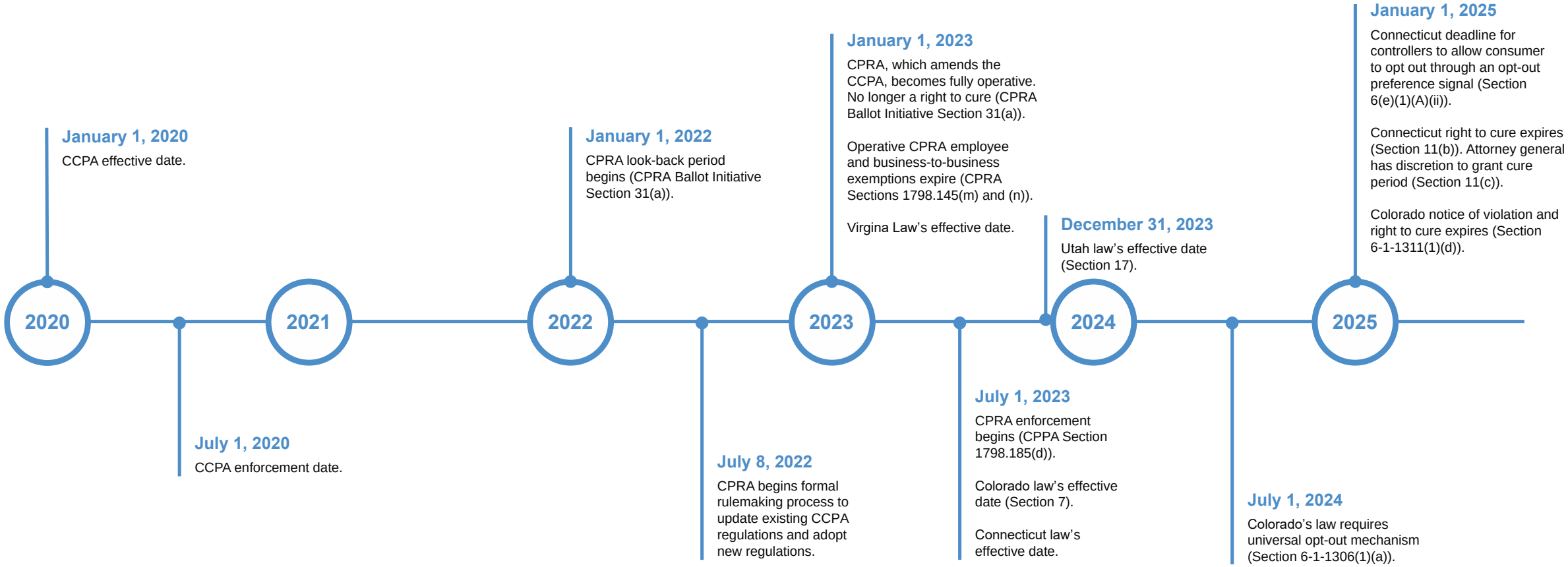
California Consumer Privacy Act – CCPA - (Passed NOV 2020 – Effective Date: CURRENT)

California Privacy Rights Act – CPRA – (Passed JAN 2021 – Effective Date: JAN 2023)

Data Privacy Institute (DPI): CPRA 2023 Checklist and Client Questionnaire

This document should not be considered legal advice and should not be used in the determination of compliance or adherence to CCPA or CPRA, it is information and intended to be an overview and guide for businesses to use in assisting with compliance efforts. For questions please contact Data Privacy Institute and info@dataprivacyinsitute.org.

Data Privacy Institute (DPI): Key Dates for Data Privacy Compliance



What do I have to do first?

- Determine if you need to comply and what sections of the CPRA apply to you.
- See what actual data is collected throughout the entire organization of all consumers and employees and vendors.
- Notification and consent documents (Website and internal).
- Data Subject Access Request (DSAR) system. Authentication and record keeping.
- Internal documents (IT/Security, CyberSecurity, Training manuals, breach docs, DPA's)
- Global Privacy Control recognition and update.
- Ensure employee (applicants, contractors, vendor data) privacy rights are clearly integrated with consumer CPRA rights.

Does My Company Need to Comply?

The CPRA applies to certain entities that process Californians' personal information. It takes effect on January 1, 2023 although the CCPA continues to apply until that time.

1. Is your organization operated for the profit or financial benefit of its shareholders or other owners?
    a. Yes - Proceed to the next question.
    b. No - The CPRA does not apply.
2. Does your organization conduct business in the state of California or with people in California?
    a. Yes - Proceed to the next question.
    b. No - The CPRA does not apply.
3. Does your organization collect consumers' personal information (EX: PII includes IP address, biometrics, email, video, device info)
    a. Yes - Proceed to the next question.
    b. No - The CPRA does not apply unless you are based in CA with CA-based employees.

If you have answered **YES** to all questions 1-3, your organization must comply with the CPRA. If not, please continue on to questions 4-6.

Starting in January of 2023, the CPRA extends the rights given to consumers to employees and applicants personal data.

Does My Company Need to Comply?

4. Does your organization have $25 million or more in gross revenue in the preceding calendar year?
    a. Yes – The CPRA applies.
    b. No – Proceed to the next question
5. Does your organization buy, sell or share the personal information of 100,000 or more consumers or households in a year?
    a. Yes – The CPRA applies.
    b. No – Proceed to the next question.
6. Does your organization derive 50% or more of its annual revenue from selling or sharing consumers' personal information?
    a. Yes – The CPRA applies.
    b. No – The CPRA may not apply.

7. Is your organization based in CA or have CA based employees and meet any one of the criteria above (Questions 4-6)?
    a. Yes – The CPRA applies.
    b. No – The CPRA may not apply.

*If you have answered **YES** to one or more of questions 4-7, your organization must comply with the CPRA.*

Does My Company Need to Comply?

- If your company has gross revenues in excess of $25m in a calendar year and you are based in CA you will have to comply with CPRA. Consumer and business data privacy rights.
- If your company has gross revenues in excess of $25m in a calendar year and you collect, use or share personal data of CA consumers you will have to comply with CPRA.
- If your company is based in CA and meet any of the criteria (+$25m in annual revenue, collect +100,000 names, 50% revenue from data sales) you must comply with CPRA.
- Employees based in CA that work for companies that meet CPRA criteria enjoy the same data rights as consumers. ALL employee data and communications are now subject to updated privacy protection rights.

Internal Data Privacy Program and Procedures

Data Privacy Program Set-up and Compliance Program Development

- Identify resources and personnel that can set-up and maintain Data Privacy Programs internally
- Invest in necessary training, education and infrastructure to continually maintain and update Data Privacy Program
- Understand the inherent risks associated with non-compliance and mitigate current data collection and usage programs

Data Mapping and Data Flow Analysis

- Inventory of all types and sources of data that hold personally identifiable information on consumers, employees, applicants, vendors and contractors
- Include all fields of data held, where they are stored (digitally, hard copy, etc.), level of accessibility, transferability, structure of data, and how the data flows throughout the organization
- Number of consumers whose personal information is being processed
- Categories of personal information collected from consumers
- Business purpose(s) for processing this information
- Source(s) of personal information
- Third parties and service providers with which your organization shares, sells, or discloses personal information
- Categories of personal information that are being sold, shared, or disclosed

Internal Data Privacy Program and Procedures

Data Classification and Usage Analysis

- Once data map and inventory have been completed, data owner must review stored fields of data to determine sensitivity levels.
- Classify special fields of Personally Identifiable Information (EX: biometrics, ethnicity, health data, etc.)
- Where necessary ensure additional measures be taken with Specially Classified Data Fields and Personally Identifiable Information.
- Redaction and disclosure and lawful use analysis along with additional disclosures.

Update all Privacy Policies, Disclosures, Terms and Conditions and Consents to comply with CPRA 2023

Privacy Policy and Notice

Does your organization's privacy notice:

- List the categories of personal information and sensitive personal information collected or used;
- List the categories of sources from which that information is collected;
- Describe the purposes for which the information is collected and used;
- Outline the length of time that the business intends to retain each category of personal and sensitive personal information;
- List the categories of information sold, shared, or disclosed for a business purpose, and the purpose for doing so;
- Explain the categories of third parties to whom information is disclosed;
- Discuss consumer rights under California law, and provide 2 or more methods for consumers to exercise those rights.

And:

- Is your organization's privacy notice updated at least every 12 months?

*If you answered **NO** to any or all these questions, you will need to update your privacy policies and notices.*

Data Subject Access Requests (DSAR)

Access requests

• Do you have two or more methods through which consumers can submit access requests (potentially including a toll-free telephone number)?
• Does your organization have mechanisms in place to verify the identity of people requesting information?

*If you answered **NO** to either of these questions, you will need to develop processes with respective policies related to consumer access requests or implement a DSAR platform. These are similar requirements in the EU's General Data Protection Regulation (GDPR).*

Selling Personal Information

Does your organization sell personal information?

If you answered **yes,** consider the following questions:

- Is there a clear and conspicuous link on your Internet homepage titled, “Do Not Sell or Share My Personal Information”?
- Are mechanisms in place to respond, and limit the disclosure of data?
- Can personal information be deleted in response to a deletion request?
- Are appropriate mechanisms in place to ensure the requested information is deleted from their records?
- Have all service providers and/or contractors (as defined by the CPRA) been identified?
- Are appropriate contracts in place?

*If you answered **NO**, your organization should review its data mapping initiatives and contracts.*

Implement processes and technical measures to secure personal information

- Are there processes in place to keep personal information accurate, correct, and up to date?
- Is personal information stored in a confidential and safe manner (whether physically or electronically)?
- Can personal information be pseudonymized, anonymized, deidentified, or aggregated?
- Can personal information be encrypted or redacted?
- Are IT systems and services regularly tested for security vulnerabilities or enhancements?
- Has your organization implemented a risk control or security management framework?

*If you answered **no**, you will need to set up an overall information security policy/implement security management framework. Implementing an ISMS (information security management system) that conforms to the international standard ISO/IEC 27001:2013 is highly recommended.*

Data Breach and Data Security Incidents

Data breach notification

- If your organization suffers a data breach, do you have a mechanism to notify affected CA residents?
- Does the notification form include all the requirements listed in Cal. Civ. Code § 1798.82(d)?

*If you answered **no**, you will need to develop policies and procedures related to incident response and data breach notification.*

Data Privacy for Minors

Children's data

• Are appropriate opt-in mechanisms in place regarding the selling or sharing of children's data, age 13 to 16?

*If you answered **no**, you will need to set up a policy and supporting processes to obtain valid opt-in before processing children's personal information.*

Employee Training and Education

Ensure your employees are trained and competent

Any staff involved in processing personal information must understand the CPRA's requirements and know how to maintain good data hygiene.

• Do all employees understand the importance of protecting personal information, basic CPRA principles, and the procedures to ensure compliance?
• Are all individuals responsible for managing consumer inquiries trained on consumer rights under the CPRA and how to respond to consumers?

*If you answered **no**, you will need to set up a training and awareness program so that all staff responsible for handling consumer inquiries related to privacy are trained on the CPRA generally, consumer rights specifically, and your organization's processes for managing and responding to consumer requests for information.*

Program and Compliance Monitoring

Monitor and audit compliance

Complying with the CPRA is an on-going process. Periodic internal audits will ensure your activities remain up to date and that you will not fall out of compliance. You should:

- Schedule regular audits of personal data processing activities and security controls
- Keep records of personal data processing up to date
- CPRA requires a 2 year record keeping period for all DSAR requests and outcomes

Data Collection for Marketing Purposes

CPRA and marketing

Will you be collecting data for marketing purposes?

- Direct mail
- Email marketing
- SMS or Mobile
- Social media marketing
- Ethnic or segmented marketing
- Newsletters or Targeted Content
- Website, Digital Advertising

*If you answered **yes**, then **data processing agreements** (DPA's) will need to be in place with all third parties that provide processing/collection services. Terms and conditions as well as all privacy policies will need to be updated accordingly to comply with CPRA. Specially protected data fields will require a higher level of protections and rights. DSAR rights for consumers and employees must be implemented.*

Data Retention and Minimization

Data Minimization

- Any data and information collected must be “reasonably necessary and proportionate” for the purposes for which it was collected or for another “disclosed purpose” similar to the context under which it was collected.
- Data can not be utilized except for “permitted uses” and the data can not be used in alternate ways unless parties are notified and consent has been given for the new purposes.

Collected data can and should be kept for only as long as necessary to perform the outlined functions and a data retention strategy must be developed and implemented for all classes of Personal Information collected.

Additional Data Privacy Considerations

Transactional Data, Rewards & Loyalty Programs and Specially Protected Fields

Do you collect and use transactional data?

Do you have a loyalty rewards program that has Personally Identifiable Information stored or utilized?

Do you collect internal information on employees? Health or other special PII (vaccination status, biometrics, etc).

*If you answered **yes** to any of the questions above, then DPA's will need to be in place with all third parties that provide processing/collection services. Terms and conditions as well as all privacy policies will need to be updated accordingly to comply with CPRA. Health and biometric data are specially protected data fields and will require additional levels of protection for CPRA compliance. DSAR rights for consumers and employees must be implemented.*

NEXT STEPS

1. Update all applicable items identified on CHECKLIST.
2. Remediation of Consumer Disclosures, Terms and Conditions and Consumer Consents at all Points of Collection (POC).
3. Data mapping is required for 2022 Lookback on all data collected and used prior to CPRA 2023.
4. Implement a functioning DSAR that can track inbound requests and provide a system for remediation and flow of communications with Data Subjects, as well as authenticate all requests.
5. Ensure that Consumer and Employee Data Privacy Rights are identical starting in JAN 2023.
6. Contact Data Privacy Institute to schedule a time to talk about receiving a compliance AUDIT and final Data Privacy Compliance certification.