Littler | CPRA Compliance Suite

The California Privacy Rights Act of 2020 (CPRA) substantially expands the privacy and information security obligations of most employers doing business in California. This comprehensive legal framework applies to the personal information of California residents who are employees, job applicants, independent contractors, and board members, and employees' dependents who receive benefits through the employer (collectively, "HR Individuals"). In a marked departure from previous U.S. laws related to the data of HR Individuals, the CPRA creates a comprehensive data protection regime similar to data protection laws in many other parts of the world, such as the European Union's General Data Protection Regulation.

This dramatic expansion of employers' data obligations went into effect on January 1, 2023 and requires significant changes to existing policies, procedures, and practices for handling HR Individuals' personal information. Enforcement began on July 1, 2023.

Our Littler Insight — Substantial New Privacy Obligations for California Employers: The California Privacy Rights and Enforcement Act of 2020 Passes at the Polls — provides an overview of the legislation.

The effect of the CPRA's final regulations and rule making is available in our Littler Insight — Finalization of Regulations Clears Path for Employers to Complete California Privacy Rights Act Compliance Efforts Before June 30, 2023 Deadline.

To assist your organization with CPRA compliance, Littler's CPRA team has developed the CPRA Compliance Suite. This comprehensive offering of templates and guidance can be purchased as an entire package, or on an a la carte basis.

Please contact your Littler attorney or CPRA@littler.com for more information on pricing.

Littler

Littler CPRA Compliance Team

Kwabena Appenteng
Shareholder
Chicago, IL
kappenteng@littler.com

Zoe Argento
Shareholder
Denver, CO
zargento@littler.com

Phil Gordon
Shareholder
Denver, CO
pgordon@littler.com

Andrew Gray
Associate
Austin, TX
argray@littler.com

Denise Tran-Nguyen
Shareholder
San Diego, CA
dtrannguyen@littler.com

As outlined in further detail below, Littler's CPRA Compliance Suite includes (1) Human Resources Data Materials, (2) an Information Security Supplement, and (3) a Non-HR Data Supplement.

1. Human Resources Data Materials:

- **CPRA for Employers White Paper:** A 17-page white paper covering key points on the CPRA's application to human resources data, including advice on practical steps for compliance. This item is free with any purchase from the CPRA Compliance Suite.
- **Project Plan:** A plan mapping the steps of the CPRA compliance project along with designations of responsibility.
- **Three Fact-Finding Memos:** Includes one for (a) employees; (b) applicants; and (c) other types of HR data (e.g., independent contractors, temporary workers, dependents, board members, etc.). These memos assist the Company in identifying data within scope, tracking data flow and location, and collecting the information to respond to data rights requests and draft the privacy policies.
    - Each fact-finding memo is 30+ pages with detailed checklists and explanations at each step to help users answer questions and to explain how the CPRA applies to HR data, which saves employers hours of work on analysis and brainstorming.
    - Includes tables for identifying vendors that handle California personal information and for tracking their execution of CPRA-compliant addenda to their service agreements.
- **Template Applicant Notice at Collection + Privacy Policy:** Intended for posting on the Company's career website and other sites where applicants begin the application process.
- **Template Employee and Other HR Notice at Collection + Privacy Policy:** Intended for posting internally. In addition to employees, this document covers independent contractors, temporary workers, board members and directors, dependents, spouses, and emergency contacts.
- **CPRA Vendor Agreement:** Addendum to modify a vendor service agreement to add the provisions required by the CPRA. Intended for employer to propose to vendors. Version for vendor to propose to an employer available on request.
- **Internal Data Rights Policy:** A policy and set of procedures and administrative forms for responding to data rights requests. The policy includes but is not limited to designations of responsibility, request processing procedures, a request tracking process, the scope of each data right, grounds for rejecting each right, administrative requirements and deadlines, and forms, e.g., forms for submitting a request, forms for acceptance/rejection, and forms for notifying of 45-day extension to respond.
- **HR Data Retention Policy:** Covers issues including purging, litigation holds, and responsibilities.
- **HR Data Retention Schedule:** A federal + 50 states retention schedule with a decision tree to help you decide (a) what requirements to prune based on states, employee categories, industry, etc.; and (b) what requirements to extend based on specific statutes of limitation/types of lawsuits for which having more data would significantly reduce risk.
- **Training PowerPoint:** Detailed PowerPoint presentation on managing data rights requests, negotiating CPRA contracts with vendors, and managing notices.
- **Training Session:** A one-hour training by Littler including responding to questions from the Company's personnel and running through hypotheticals.

2. Information Security Supplement:

The CPRA grants California residents a right to recover up to $750 in statutory damages, on an individual or class-wide basis, for a data breach resulting from the Company's failure to institute reasonable safeguards. Implementing written information security policies and a security incident response plan, to the extent not already in place, or enhancing existing policies or plans to more specifically address HR data, should decrease the risk of a data breach, bolster the Company's argument that it maintains reasonable safeguards, and better prepare the Company to respond to security incidents.

- Information security policies and procedures
- Security incident response plan

3. Non-HR Data Supplement:

- **Project Plan:** A plan mapping the steps of the CPRA compliance project, along with designations of responsibility. This project plan can be combined with the project plan addressing HR data.
- **Fact-Finding / Data-Mapping:** Memos and spreadsheet to assist the Company in identifying non-HR data within scope, tracking data flow and location, and collecting the information to respond to data rights requests and draft the privacy policies. The documents include tables for identifying vendors that handle California personal information and for tracking their execution of CPRA-compliant addenda to their service agreements.
- **Notices at Collection / Privacy Policies:** Template website privacy policy intended to meet both the CPRA's notice at collection requirement and the CPRA's privacy policy requirement for non-HR data.
- **CPRA Vendor Agreement:** Addendum to modify a vendor service agreement to add the provisions required by the CPRA.
- **Internal Data Rights Policy:** A policy and set of procedures for responding to data rights requests regarding non-HR data, and administrative forms.
- **Training Session:** Training session for individuals managing data rights requests, negotiating CPRA contracts with vendors, and managing notices regarding non-HR data.

For more information, contact us at CPRA@Littler.com or go to https://www.littler.com/cpra.