CCPA/CPRA Compliance and Data Inventory Management Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The California Privacy Rights Act (CPRA), an evolution of the CCPA, marks a monumental shift towards enhanced consumer data privacy and data sovereignty in the United States, mandating rigorous operational and technical compliance for any business processing the personal information of California residents. CCPA/CPRA Compliance and Data Inventory Management Training Course provides an essential, actionable roadmap for organizations to navigate the complexities of this evolving regulatory landscape. Key focus areas include mastering the expanded consumer rights, establishing robust Data Subject Access Request workflows, and implementing a sustainable Data Inventory Management system the foundational pillar of any mature privacy program. Non-compliance carries severe financial and reputational risk mitigation consequences, making this investment in privacy upskilling absolutely critical for operational resilience in the digital economy.

This course is engineered for immediate, real-world application, transforming regulatory requirements into practical, day-to-day business processes. It emphasizes the crucial link between legal mandates and data governance best practices, particularly through the lens of data mapping and data lineage to maintain continuous compliance. Participants will learn to move beyond basic regulatory adherence to build a proactive, privacy-by-design culture. By leveraging innovative privacy technology and structured data lifecycle management, this training ensures your organization not only meets its legal obligations but also cultivates customer trust and strengthens its overall data security posture against emerging threats in cross-context behavioral advertising and Automated Decision-Making Technology.

Programme Curriculum

CCPA/CPRA Compliance and Data Inventory Management Training Course

Introduction

The California Privacy Rights Act (CPRA), an evolution of the CCPA, marks a monumental shift towards enhanced consumer data privacy and data sovereignty in the United States, mandating rigorous operational and technical compliance for any business processing the personal information of California residents. CCPA/CPRA Compliance and Data Inventory Management Training Course provides an essential, actionable roadmap for organizations to navigate the complexities of this evolving regulatory landscape. Key focus areas include mastering the expanded consumer rights, establishing robust Data Subject Access Request workflows, and implementing a sustainable Data Inventory Management system the foundational pillar of any mature privacy program. Non-compliance carries severe financial and reputational risk mitigation consequences, making this investment in privacy upskilling absolutely critical for operational resilience in the digital economy.

This course is engineered for immediate, real-world application, transforming regulatory requirements into practical, day-to-day business processes. It emphasizes the crucial link between legal mandates and data governance best practices, particularly through the lens of data mapping and data lineage to maintain continuous compliance. Participants will learn to move beyond basic regulatory adherence to build a proactive, privacy-by-design culture. By leveraging innovative privacy technology and structured data lifecycle management, this training ensures your organization not only meets its legal obligations but also cultivates customer trust and strengthens its overall data security posture against emerging threats in cross-context behavioral advertising and Automated Decision-Making Technology.

Course Duration

10 days

Course Objectives

1. Master the latest CPRA amendments and their impact on existing CCPA compliance strategies.
2. Delineate the expanded definitions of Sensitive Personal Information (SPI) and its specific handling requirements.
3. Implement a repeatable, scalable Data Inventory and Mapping process for full data visibility and data lineage.
4. Architect efficient, legally sound workflows for handling all types of Data Subject Access Requests
5. Develop compliant notices, including the Right to Opt-Out of Sharing for cross-context behavioral advertising.
6. Analyze the criteria for the new California Privacy Protection Agency (CPPA) enforcement and risk mitigation strategies.
7. Establish clear data retention, minimization, and disposal policies to comply with data lifecycle management.
8. Evaluate vendor and third-party risk through stringent service provider contracts and privacy diligence.
9. Apply the Privacy by Design and Privacy by Default principles to new product and service development.
10. Conduct effective Data Protection Impact Assessments and Risk Assessments as required by CPRA.
11. Understand the CPRA's new requirements for the use of Automated Decision-Making Technology and profiling.
12. Leverage Privacy Enhancing Technologies to enhance data utility while maintaining regulatory compliance.
13. Drive organizational privacy awareness and accountability to foster a sustainable data governance culture.

Target Audience

1. Privacy and Compliance Officers

2. Data Protection Officers and Data Governance Managers
3. Legal Counsel and Attorneys specializing in technology and regulatory law
4. Information Security and IT Managers
5. Marketing and Advertising Executives involved in consumer data sharing/selling
6. Product Managers and Engineers responsible for Privacy by Design implementation
7. Internal Auditors and Risk Management Professionals
8. Heads of Customer Relations and Operations who handle DSARs

Course Modules

Module 1: CCPA to CPRA: The Regulatory Evolution

- CCPA and CPRA's new rights, thresholds, and enforcement.
- Understanding the scope
- The role and authority of the new California Privacy Protection Agency
- Increased penalties and the elimination of the 30-day "cure period."
- Defining and managing Sensitive Personal Information
- Case Study: Analysis of a CPPA enforcement action against a large retailer for failing to honor global opt-out signals, focusing on the financial penalty post-cure period removal.

Module 2: Foundational Data Inventory and Data Mapping

- Principles of data discovery and building a comprehensive data inventory register.
- Techniques for mapping data flows.
- Identifying categories of Personal Information and their business purposes.
- Documenting data retention schedules and legal bases for processing.
- Tools and technologies for automated Data Mapping
- Case Study: Demonstrating a successful Data Mapping project post-acquisition, highlighting how the inventory uncovered high-risk shadow IT systems.

Module 3: Expanded Consumer Rights: Access and Correction

- Implementing the Right to Know requirements and data portability.
- Operationalizing the new Right to Correct inaccurate personal information.
- Verification procedures for consumer identity
- Format and timeliness requirements for request fulfillment
- Handling complex requests involving multiple data systems.
- Case Study: Simulating a "Right to Correct" request where a customer disputes inferred data points used for profiling and the steps taken to validate and update the information.

Module 4: The Right to Delete and Data Minimization

- Processing the Right to Delete and managing exceptions to deletion.
- The concept of Data Minimization and its strategic importance to CPRA.
- Technical methods for secure and permanent data erasure across all environments.
- Notifying third parties and service providers of a deletion request.
- Establishing a periodic review for data that is no longer necessary.
- Case Study: A multinational company's challenge in securely deleting customer data stored across various cloud and legacy on-premise systems to meet a deletion request.

Module 5: Opt-Out of Selling and Sharing

- The critical distinction between "selling" and the new concept of "sharing".
- Implementing the Right to Opt-Out of Sale/Sharing via a compliant link/mechanism.
- Recognizing and honoring Global Privacy Control signals.
- Requirements for handling minors' data
- Legal obligations for third parties who receive personal data.
- Case Study: Examination of a company's non-compliant cookie banner and opt-out mechanism, and the remedial steps taken to honor GPC signals and clearly present "Do Not Share" options.

Module 6: Sensitive Personal Information and the Right to Limit

- Comprehensive review of the specific categories that constitute SPI.
- The operational necessity of the Right to Limit the Use and Disclosure of SPI.
- Technical controls and access restrictions for SPI in databases and systems.
- Displaying the 'Limit the Use of My Sensitive Personal Information' link.
- Balancing SPI use with necessary business operations and security
- Case Study: A healthcare-adjacent fitness app handling biometric and geolocation data; detailing the system architecture changes required to implement the "Right to Limit" on sensitive health information.

Module 7: Privacy Policy and Consumer Notice Requirements

- Mandatory content elements for a CPRA-compliant Privacy Policy.
- Rules for a compliant Notice at Collection
- Transparency requirements regarding data retention periods and deletion rights.
- Best practices for accessibility and clarity in privacy notices.
- Translating technical data practices into plain, consumer-friendly language.
- Case Study: Redrafting a vague privacy policy to meet the CPRA's explicit disclosure requirements for categories of PI collected, sold, or shared, including retention periods.

Module 8: Data Protection Impact Assessments and Risk

- When and how to conduct a mandated Data Protection Impact Assessment or risk assessment.
- Methodology for identifying and scoring privacy-related risks
- Documenting mitigation measures and justifying high-risk data practices.
- Integrating DPIAs into the System Development Life Cycle
- The interplay between CPRA risk assessments and broader Enterprise Risk Management.
- Case Study: Conducting a DPIA for a new internal AI tool that profiles employee performance, focusing on mitigating discrimination and transparency risks.

Module 9: Vendor and Third-Party Risk Management

- Structuring CPRA-compliant contracts for Service Providers, Contractors, and Third Parties.
- The flow-down obligations for downstream data recipients.
- Conducting privacy due diligence and vendor risk assessments.
- Monitoring vendor compliance and enforcing contractual terms.
- Impact of the CPRA on B2B data and employee data exemptions
- Case Study: Review of a third-party ad-tech vendor contract, identifying and correcting non-compliant clauses that failed to restrict the vendor's use of consumer PI.

Module 10: Technical Security and Breach Notification

- Understanding the CPRA's requirement for "reasonable security procedures and practices."

- Integrating CCPA/CPRA compliance into the broader Information Security framework.
- Requirements for Data Breach notification to consumers and the CPPA.
- The role of encryption and other Privacy Enhancing Technologies
- Specific civil litigation risk related to security breaches of unencrypted PI.
- Case Study: Analyzing a major data breach involving unencrypted SPI and the subsequent regulatory and civil class-action fallout under the CPRA's private right of action.

Module 11: CPRA and Automated Decision-Making Technology (ADMT)

- Defining and identifying the use of ADMT and profiling in business operations.
- New requirements for providing notice and choice regarding ADMT use.
- Understanding the right to opt-out of ADMT for significant decisions.
- The need for human review and transparency in profiling activities.
- Integrating ADMT compliance into the Privacy by Design process.
- Case Study: Reviewing a credit scoring algorithm that uses ADMT, detailing the steps required to provide the consumer with meaningful information about the logic involved and the right to opt-out.

Module 12: Employee and B2B Data Compliance

- The expiration of temporary exemptions for Employee and Business-to-Business data.
- Applying consumer rights to employee and job applicant data.
- Strategies for collecting and managing employee personal information compliantly.
- Extending data inventory and mapping to include HR and B2B data systems.
- Updating internal policies and training for employee data handling.
- Case Study: Drafting an internal Notice at Collection for new employees and job applicants, ensuring full compliance with their CPRA rights.

Module 13: Operationalizing Data Subject Access Requests

- Designing an end-to-end DSAR workflow for efficiency and compliance.
- Developing a strong consumer request portal and communication strategy.
- Leveraging Privacy Technology to streamline fulfillment.
- Tracking, reporting, and auditing the DSAR process for accountability.
- Managing simultaneous or complex requests
- Case Study: Modeling a high-volume DSAR submission scenario and using a privacy workflow tool to automate identity verification, data retrieval, and final response generation within the 45-day window.

Module 14: Building a Culture of Data Governance

- Implementing Privacy by Design and Default in product development.
- Creating a multi-disciplinary Data Governance Committee structure.
- Developing role-based training and certification programs for all employees.
- Measuring and reporting on key privacy metrics and compliance health.
- Establishing a periodic audit and self-assessment program for continuous compliance.
- Case Study: Implementing a Privacy Champions program across different business units to decentralize ownership of data privacy and foster a culture of vigilance.

Module 15: Global Privacy Intersections and Future Trends

- Contrasting CPRA with other major regulations
- Impact of emerging federal privacy legislation in the United States.

- Monitoring the CPPA?ÇÖs ongoing rulemaking
- Future trends: Data Localization, Privacy-Preserving Computation, and Decentralized Identity.
- Preparing for the next wave of state and international privacy laws.
- Case Study: Analyzing a scenario where a business must comply with both CPRA and GDPR for the same consumer and the resulting joint compliance strategy.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com