Informatica

Executive Brief

Data Privacy by Design: California Consumer Privacy Act

Key Statistics

- 69% of global consumers are prepared to boycott any company they believe does not take data protection seriously
- 62% blame the company first in the event of a data breach, rather than the hacker
- 83% of US consumers will stop spending for several months after a breach or serious incident
- 21% of US consumers will never return to a brand that has suffered a data breach[1]

Drive Compliance Readiness to Support Customer Trust and Reduce Organization Risk

California Residents Get Control of Their Personal Information and Set Expectations for Privacy

The California Consumer Privacy Act (CCPA) joins a growing movement of worldwide privacy legislation designed to provide privacy rights to individuals and to give them greater control over the use of their personal information.

The CCPA grants consumers rights for their personal data and prevents businesses from discriminating against them for exercising those rights. In particular, consumers can ask about the categories and specific pieces of personal information a business has collected about them and the purposes for which the business uses that information. Consumers can ask the business to delete personal information it has collected about them or request that their personal data not be sold to third parties. The CCPA also obligates businesses to implement and maintain reasonable data security procedures and policies appropriate to the nature of the information. It also creates a private right of action (with potentially high liability for businesses) for any breaches of that obligation that result in unauthorized access to personal information covered by California's breach notification law.

Key Considerations for Data Privacy

Privacy officers and security teams need automated tools to effectively manage data privacy readiness. Unfortunately, privacy officers are often frustrated by the inability to identify, locate and assess personal information, facilitate cooperation and collaboration among business, privacy and IT, and to effectively protect and monitor personal information.

Informatica® data privacy solutions are designed to provide a foundation that supports data privacy regulations and consumer trust. By proactively managing compliance requirements, organizations can ensure that data risks (such as data misuse or loss) are remediated and monitored, and that stakeholders can effectively collaborate for privacy readiness, audits, and reporting.

[1] https://www.infosecurity-magazine.com/news/fifth-consumers-never-return

Informatica data privacy solutions provide organizations with the ability to continuously (1) Manage data governance policies (2) Discover and manage personal and sensitive data (3) Map individual identities to their personal data (4) Analyze and track data risks (5) Take action to protect personal information and manage data subject and consent requests, and (6) Track privacy progress, communicate privacy actions and status.

To meet the challenges of CCPA, organizations need better intelligence and personal data security to provide residents of California (CA) the control and protection required by the CCPA. The table below reviews key data-intelligence and security issues that should be addressed to help support CCPA compliance:

Data Privacy Needs	Outcomes
1. Determine How Our Organization Processes CA Personal Data (Data governance policies)	• Create definitions that encompass CA resident personal data • Define what data is collected and how the data will be used
2. Where Is CA Personal Data? (Discover and classify personal data)	• Precisely locate and map where CA resident personal data is held, particularly with respect to data that is subject to breach notification under CA law
3. Create Identity Registry (Link CA identities to their personal data)	• Support rapid response on rights requests by CA residents • Quickly reference where data is distributed in an organization
4. Determine How CA Personal Data is Protected (Analyze CA residents data security risk)	• Understand where CA resident data is at risk for misuse or unauthorized access, prioritize and plan remediation, particularly with respect to data that is subject to breach notification under CA law • Identify the security needed for different types of CA resident data
5. Protect CA Personal Data and Respond to Request Rights Requests (Data security, rights processing)	• Support requests for deletion and sale of data • Protect CA resident data in operations, development and test and analytics
6. Track Progress and Understand the Current State of CCPA Privacy Readiness (Measure, communicate, collaborate)	• Respond to status requests • Track CCPA program progress

About Informatica

Digital transformation changes expectations: better service, faster delivery, with less cost. Businesses must transform to stay relevant and data holds the answers.

As the world's leader in Enterprise Cloud Data Management, we're prepared to help you intelligently lead—in any sector, category, or niche. Informatica provides you with the foresight to become more agile, realize new growth opportunities, or create new inventions. With 100% focus on everything data, we offer the versatility needed to succeed.

We invite you to explore all that Informatica has to offer—and unleash the power of data to drive your next intelligent disruption.

Powered by AI and the industry's leading intelligent data platform, Informatica data privacy provides capabilities to support data-centric tenets of the CCPA:

1. **Define and Manage Governance Policies**

   Data Governance to define, document and measure both business and technology policies, responsibilities, processes, and data terms. With the Axon™ governance task framework and visual workflows, organizations can identify critical business user stakeholders and align them with the data and processes they own.

2. **Discover, Classify, and Understand Personal and Sensitive Data**

   Leverage AI to provide an enterprise view and analysis of personal information assets and metadata so organizations can rapidly locate, classify, and understand all their data environments; multi-cloud, Hadoop, relational and file storage systems, and both unstructured and structured data.

3. **Map Identities**

   Data subject registry links identities to personal data, so organizations can quickly determine what personal data belongs to which individual (customer, employee, etc.). This provides support for data subject access rights and integrates to consent management systems.

4. **Analyze Data Risk, Establish Protection Plans**

   Analyze personal information risk (likelihood of misuse or loss) and provides customizable risk impact models, so organizations can prioritize remediation and effectively deploy resources and investments. Risk is continuously measured and recorded to provide Key Risk Indicators for privacy and protection programs.

5. **Protect Data, Manage Subject Rights and Consent**

   Anonymize and pseudonymize personal information to ensure that organizations control the access and viewing of customer and employee personal information. Create a 360-degree view of data subjects and consents by capturing and documenting lineage, history, and data retention periods, while supporting data subjects' rights through workflows and actions.

6. **Measure, Communicate, Audit Readiness**

   Rich visualizations provide global intelligence to support decision makers, detailed views for practitioners, and immediate detail on personal information to support audit requirements to manage and track privacy and protection programs.

Informatica

Worldwide Headquarters 2100 Seaport Blvd., Redwood City, CA 94063, USA Phone: 650.385.5000, Toll-free in the US: 1.800.653.3871

IN08_0419_03601