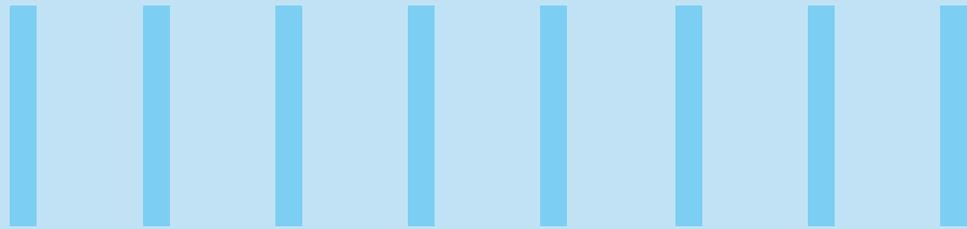




## ARE YOU TRULY CCPA COMPLIANT?

A quick health check





## Introduction

With the increased awareness amongst consumers regarding the collection and usage of their personal information by companies, there is greater focus on data privacy and security. To mitigate the challenges arising from this focus and provide more control to consumers over their data, California Consumer Privacy Act 2018 was passed by the State of California on 28th June 2018 and came into effect on 1st January 2020.

Even though companies have been actively preparing to comply with CCPA requirements, they still have a long way to go. A comprehensive solution can not only help achieve this compliance, but it can also enhance consumer confidence in the brand, increase the amount of data consumers are willing to share, and thus help expand data-based research and products.

This document helps companies evaluate their level of readiness with respect to requirements under CCPA. It provides a comprehensive list of best practices required by companies for a robust compliance solution based on our extensive experience.

So read on and perform a health check!

## Key Competencies:

The following have been identified as the key competencies that organizations need to develop policies on and implement solutions to comply with CCPA.

- Know your data
- Consumer rights management
- Vendor contract management
- Policy management
- Data retention and archival mechanism
- Training and awareness
- Monitoring mechanism
- Legal reporting

## Know your data:

This is an important step to be undertaken at the beginning of your compliance journey. Knowing your data or personal data discovery helps the organization understand their data landscape and identify the 'what' and 'where' aspects of personal information in their applications and systems.

- Do you have the list of personal information elements that can be used to identify an individual, collected and stored with your organization?
- Have you identified the personal information elements which in combination with others can be used to identify an individual?
- Have you discovered this personal information in your applications and categorized them as per sensitivity?
- Have you developed an application inventory and summary view to identify impacted applications/databases?
- Has this been vetted by legal or your data privacy office (DPO) team?

## Consumer rights management:

The major objective of CCPA is to provide consumers with certain rights that grant them more information and control over their personal information. Hence,

the fulfillment of these rights becomes a significant capability required for organizations.

- Have you defined clear roles and responsibility for request fulfillment?
- Have you established processes to fulfill consumer rights?
- Are these processes automated to ease the fulfillment of consumer rights?
- Have you established an automated customer verification process and collect data points to validate customer identity?
- Have you defined workflows to track SLA for submitted requests?
- Do you maintain audit trails for request fulfillment for audit purposes?
- Do you send automated emails to customer and fulfillment teams for confirmations, clarifications, SLAs, etc.?
- Do you have a data repository or a data store that maintains all personal information to fulfill consumer rights?
- Does this datastore contain all information related to data sources and personal data elements?

## Vendor Contract Management:

Organizations engaging in the collection, disclosure, or sale of personal information with vendors / third parties or service providers are required to establish processes for adherence to CCPA requirements by the contracted parties.

- During the vendor onboarding process, do you collect documentary evidence for privacy notice disclosures and privacy regulatory compliance?
- Does your vendor contract incorporate clauses required for CCPA compliance by the vendor such as ones listed below?
  - Support needed for fulfillment of CCPA rights
  - The purpose of sharing the information and refrainment from

using for any other purpose

- Liability in case of breach or violation
- Data security measures
- Do you have a process to audit vendor practices for CCPA compliance?
- Do you have a termination policy/ clause in case of repeated violation of CCPA?

## Policy management:

Even though organizations display a privacy policy, they may not be fully compliant with CCPA. Following are some of the definitive points that organizations need to observe:

- Do you provide CCPA privacy notice to the consumer at the point of personal data collection (for both online and offline data collection)?
- Does your privacy policy explain how to submit a request under the CCPA and provide at least two ways for submission of the request?
- Do you disclose categories of personal information collected and the purpose of collection?
- Do you disclose whether the organization sells or does not sell personal information and provide an opt-out option in case it is sold?
- Do you provide a separate link for CCPA privacy notice and update it annually?

## Data retention and archival mechanism:

As per CCPA, data should be retained by organizations only for the period it is required, post which it should be disposed of. A holistic data retention policy based on various regulatory requirements is required to trigger data disposal.

- Have you formulated a data retention policy for various data categories?
- Do you have a defined RACI to operationalize the data retention policy?

- Have you defined business rules to operationalize retention policy?
- Have you developed an ILM solution for retention policy implementation?

## Training and Awareness:

In addition to implementing an end-to-end solution, it is imperative that organizations create awareness about data privacy and CCPA requirements amongst its staff members and train them to handle CCPA queries.

- Have you developed training content for front desk executives to handle CCPA related queries?
- Have you developed SOP for rights fulfillment?
- Do you make use of flyers, emailers and audio-visual content to spread CCPA awareness across the organization?

## Monitoring mechanism:

Organizations need to establish an ongoing monitoring mechanism to ensure the CCPA compliance processes in place are adopted and adhered to by their teams.

- Have you established a Data Privacy Impact Assessment (DPIA) process for an audit?
- Do you have a clearly defined RACI to perform the audit?
- Do you conduct or have a defined plan to conduct DPIA periodically (once a year), or on the adoption of new/change in business products/process or violation of regulation?
- Do you have validation and sign off strategy for privacy risk mitigation and acceptance by the compliance team?

## Legal Reporting:

CCPA imposes penalties in case of violations if they are not cured within 30 days of notification. Also, it is good to have a view for the organizations on the various parameters related to CCPA compliance which can be used for external audits or as proof of compliance with Government authorities.

- Do you have a reporting dashboard to get a quick view of various CCPA requests received and serviced?
- Are you able to track the various metrics related to the service of requests?
- Do you have a breach monitoring mechanism and able to track the breach response/resolution through a central dashboard?
- Do you have a view of the risks and issues in CCPA compliance and track the progress of their mitigation strategy/control measures?

## Summary:

The key focus areas listed in this document help an organization implement a holistic and automated process for CCPA compliance. Organizational capabilities of consumer interaction services and data access services supported by data discovery and classification, information life cycle management, data integration, and data security are required to develop a robust CCPA compliance solution.

Infosys can assist you in performing a gap assessment to evaluate your CCPA

health status. You can do a dipstick survey through our CCPA quick analysis tool. We also have a ready solution developed on ServiceNow for the fulfillment of consumer rights along with the logical data model for the CCPA data store for the storage of personal information. These can be customized as per the organizational structure and readily adopted by organizations.

Please contact us at [ccpa@infosys.com](mailto:ccpa@infosys.com) for a demo for these solutions.



For more information, contact [askus@infosys.com](mailto:askus@infosys.com)

**Infosys**<sup>®</sup>  
Navigate your next

© 2020 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.