The Most Efficient Path to Becoming CCPA Compliant

White paper

California Consumer Privacy Act or CCPA goes into effect on January 1, 2020. This act confers new rights on consumers to obtain more control over their Personally Identifiable Information (PII), how it is used, and whether it can be sold or shared by organizations. Starting January 1st 2020, companies that have gross revenue of more than $25mn, process PII for more than 50k natural persons (i), and make 50% annual from selling data must comply with the regulation. Selling data is defined as trading PII for anything of value - monetary or non-monetary. Under the new CCPA rules, businesses are required to: disclose to customers what data is collected and for what purposes, enable opt-in for minors, ensure the right to opt-out from sale , provide customers a copy of data (if requested), and delete data upon customer request. Organizations are also required to ensure that the third party vendors they work with also adhere to CCPA rules and implement measures to prevent and reduce data breach. Intentional violation of these rules can result in a fine of $7500 per occurrence while unintentional violations can cost organizations $2500. Moreover, there is no cap on these fines and the consumer also has a right to receive $100 to $750 in recourse compensation. While these rules currently go into effect for businesses with customers in California, other states are also expected to follow suit with consumer privacy rules of their own. Positioning the organization to comply with CCPA standards now will allow enterprises to meet the standards of other states that are likely to follow suit in the future. (ii)

CCPA builds on General Data Protection Regulation (GDPR) that recently went into effect in Europe. Studies show that, on average, 80% of customers are exercising their rights under GDPR. To put this in perspective, if a company only has 500 customers in California and 80% of them file a claim which is ruled to be unintentional, the resulting fines can add up to $1mn - a more expensive proposition than implementing a compliance solution. From our experience of working with different clients, Mindtree believes that organizations must follow three essential steps (see Figure 1) to become CCPA compliant

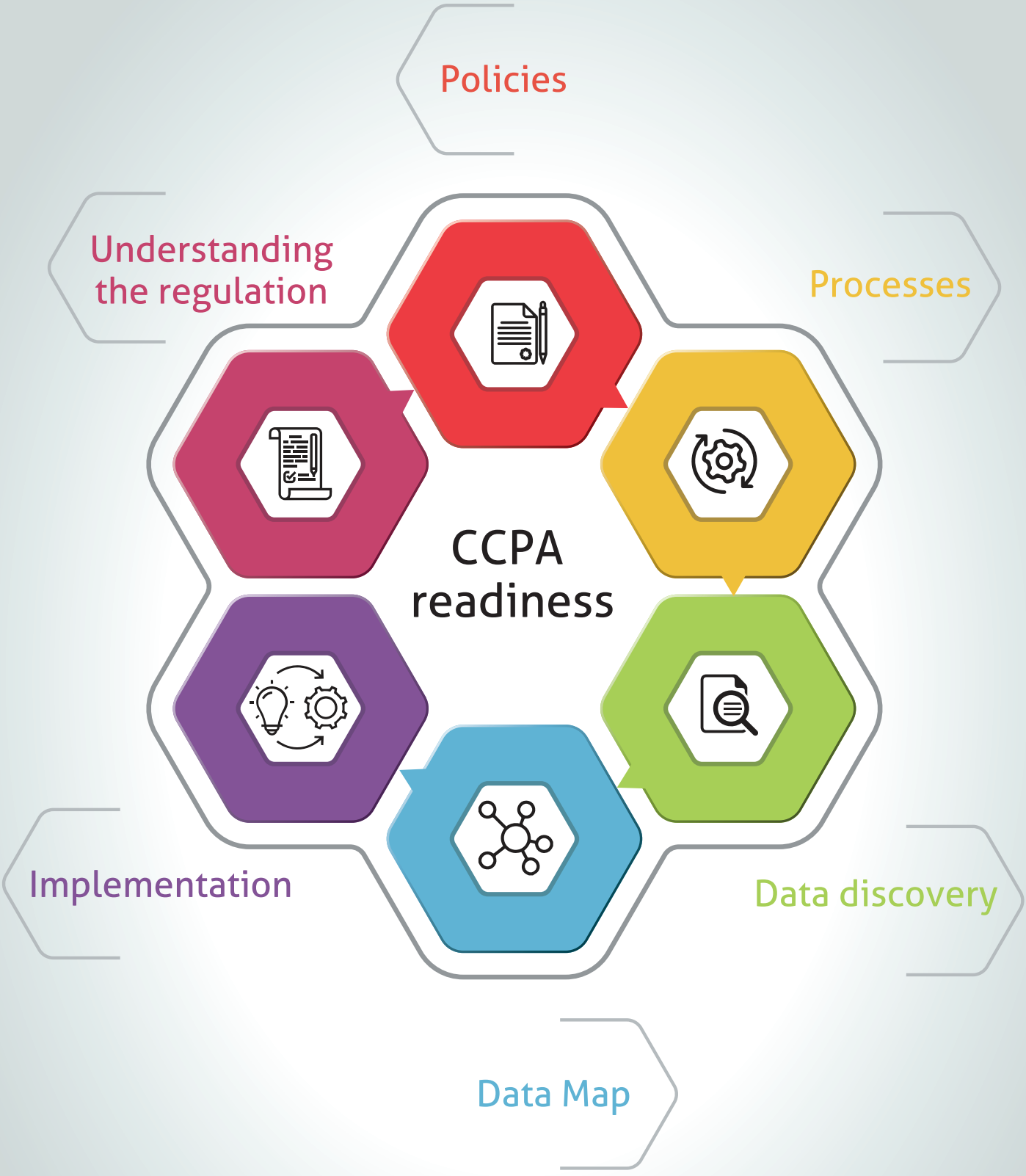

Figure 1: Steps for CCPA Compliance

1. Understand the regulation and how it applies to the organization

This step usually requires collaborating with a legal team that can help stakeholders understand the CCPA regulation and its application to the organization. In this phase, organizations should focus on:

a. Defining the policies, procedures and processes for CCPA compliance.
b. Highlighting terms and conditions and policy statements on websites.
c. Identifying changes that may be required in contracts with vendors.
d. Finalizing the data categories for which customer data is collected by the organization.
e. Communicating general awareness on CCPA in a top-down format to stakeholders to ensure they are supportive of the exercise.

2. Conduct a data discovery exercise

This phase includes identifying the applications which hold PII data within the organization's landscape.

a ***Pre-requisites –*** Obtain a list of applications and stakeholders responsible for the applications, and prepare pre-defined questionnaires customized to meet the needs of the business. The questionnaires should be reviewed/approved by the organization's legal team. A separate questionnaire is required to understand the data flow for brands. In case of organizations with multiple brands, the exercise must be conducted with business stakeholders to understand their operations and overall data flow for every brand. The next step is to create and customize the following templates.

i. ***Application Questionnaire and Personal Data Inventory –*** This questionnaire helps answer critical questions on the applications abilities, data categories, input/output to other systems and so on. The responses to these questions are necessary to defining the technical solution and identifying the required capabilities. Some of the key questions include:

- Where is the application hosted?
- What are the data subjects for the application?
- Does the application provide notice to customers?
- Is the application developed in-house or is it SaaS/third party owned?
- Who is the data controller for the application?
- Does it offer the ability to retrieve/delete data?
- Does it enable integration with other applications and data flows?
- How is the data collected and used?
- What is the data storage policy?
- What is the data retention policy?
- Is the application internal/external?
- Who has access to the application?
- What is the back-up and archival policy?

ii. ***Brand Questionnaire – T****his helps identify the data flow and processing that occurs between applications. The questionnaire gathers information from brands on the applications they use across various functions such as:*

- Customer facing – from website, stores, events, social platforms, etc.
- Order
- Loyalty
- Anonymous data
- Order fulfilment
- Interactions

iii. ***Applications List with IT and Business Owners –*** This list serves as a reference for all future purposes. Typically, the initial list is modified several times to include applications in scope and exclude others such as sunset applications or those that are not used anymore.

b *Approach –* One of the best ways to conduct the data exercise is to organize workshops of at least 90-120 minutes. During the workshops, stakeholders are walked-through the questionnaire to understand the data categories within the application, the sources the application receives data from and sends data to – in order to gain an understanding of the overall data flow. The data discovery exercise helps identify the data flow between applications, overall usage, business relevance, sharing/selling of data, and ability to store, retrieve and delete data – i.e. the key components of CCPA compliance. These sessions are also useful in addressing the questions and concerns that stakeholders may have. Additional Q&A sessions scheduled on a daily basis allow stakeholders to address their concerns and additional questions which may come up after the workshops are completed. These sessions, in addition to the workshops, help drive faster and more accurate turnarounds on the questionnaires.

c *Challenges –* During this exercise, several challenges or obstacles could arise. In some instances, organizations realize that the original list of applications that needs to be considered for CCPA has grown since the initial assessment, leading to increased scope and longer duration for the exercise. This can be addressed by staying flexible and including additional buffers to the timeline. Additional challenges may arise in the form of gaps in knowledge and undocumented transitions over time that can be resolved by working with a qualified and knowledgeable implementation partner. Commitment from stakeholders is yet another major issue. Getting C-level stakeholders such as the CIO and the DPO (Data Privacy Officer) involved, and sending multiple reminders to the stakeholders can help overcome this issue for quicker and more accurate responses.

d *Output –* This phase results in the output of several deliverables some of which are listed below:

i. Application data maps

ii. Consolidated data map

iii. Consolidated questionnaire reports

iv. Reports and insights

3. Implementation of remediation solution

This phase puts in place the processes required to meet customer requests under CCPA guidelines. The solution could range from being a manual process, or partial or complete automation - depending on the budget and timeline for implementation for the organization. Some of the components of the solution are:

a. ***User Interface or Microsites*** – Brand website can be designed to reroute customer requests to this microsite and the customer care (telephone channel) can directly access the microsite. This component helps in verifying the consumer and their details before accepting a request.

b. ***System of Record –*** This component is used for tracking, auditing and reporting.

c. ***Workflow Module –*** Involves lifecycle manage ment of a customer request across – Start, In-process, Completed, Rejected stages - and user management, including assigning tasks to different users/groups. This component enables orchestration by calling available services and triggering integrations. This component also defines the rules to determine source system integration mechanism (for notifications and escalations based on SLAs).

d. ***Data Consolidator –*** Encompasses consolidating customer records received from multiple sources and requires a consolidation tool to merge all the records in order to present a single customer view. This consolidated customer view is then shared with the Data Privacy Officer who reviews the data before sharing it with the customer.

e. ***Dashboard and Reporting –*** Involves reporting on various CCPA requests along with the current status.

Key Considerations for Success

Prior to beginning the process for CCPA compliance, there must be a commitment from top management to the project as their level of commitment will determine the effectiveness and accuracy of the discovery process. Top management must emphasize the need for and ensure co-operation with all relevant stakeholders. Even with a clear understanding of what it takes to become CCPA compliant, two of the major challenges for an organization in terms of completing this task are time and expertise. With key stakeholders involved in managing daily operations and tasks, undertaking additional responsibilities in owning their applications from CCPA perspective becomes a challenge. There is often push back, schedule conflicts, and overall resistance to participation in the process in a timely manner. This is mainly due to lack of understanding of the need for this effort or lack of desire to take on the additional responsibility that it entails. Key deliverables in the discovery phase are data maps systems, global data maps, data dictionary, data inventory, and evaluation of systems to determine CCPA compliance.

Another important aspect of the discovery exercise is review and audit of consent management and disclosures across all interfaces available to customers. The discovery phase should include a review of third party vendor contracts to ensure that the vendor is CCPA compliant. If the third party is unwilling or unable to be CCPA compliant then the organization can consider terminating the contract with the vendor.

Expertise is another important factor in implementing a solution for CCPA compliance as this is a new regulation. For an organization to gain the knowledge necessary to ensure complete compliance, outside resources will often need to provide training and this involves a learning curve. Depending on the size of the organization there could be a large number of systems that must be reviewed for accuracy. Some of these systems may be legacy systems lacking documentation, or they may have been transitioned between owners without adequate knowledge transfer, or they may simply be no longer supported. Budgetary constraints and lack of availability of experts and resources can also act as major road block to the overall process. Many organizations therefore consult with experts to complete this task. In order to find reliable third-party firms to partner with, an organization must search, vet, and review recommendations to find a good fit.

Organizations need to be aware that being compliant with CCPA regulations requires major investments in time, effort and money. The road is not easy and needs commitment from everyone in the organization - from top management to people who interact with applications and own them. Businesses/brands also need to take overall ownership and be responsible for the data they collect, how it is used, and who they share it with. CCPA ensures that there is a deep understanding of the 'why, what when, where and how' of data, enabling organizations to own their actions. It gives customers the right to question what is important, and ensures the protection of individual rights by holding organizations liable and responsible for their actions.

Mindtree as a partner

Mindtree has a significant footprint across the Retail and CPG industry in the GDPR and CCPA space. As a GDPR compliant organization, we have completed the exercise internally, and developed a framework to enable compliance with the mandate. We have also partnered with many large CPG firms and multinational corporations with multiple brands to ensure they are GDPR and CCPA compliant. We have demonstrated capabilities in interacting with all major stakeholder, providing engaging documentation and workshops that help in the development of an all-encompassing solution that ensures compliance with the regulations. Additionally, our team has created customized templates to obtain and map the origin, type, properties and flow of PII across systems as well as their attributes. We continuously refine the framework and processes to further improve efficiencies. With adequate and timely alignment from the top management at CXO level, our team has the ability to ensure that clients complete a successful compliance journey. In essence, our team brings the resources, knowledge, and personnel necessary to not only build a solution that is CCPA compliant but also deliver an exceptional customer experience.

---

i Natural person is defined as in a human being with their own personality as opposed to a legal Person which may but a public, private, or government organization

ii Tackle The California Protection Act Now Forrester Research 2019 www.forrester.com

About Mindtree

Mindtree [NSE: MINDTREE] is a global technology consulting and services company, helping enterprises marry scale with agility to achieve competitive advantage. "Born digital," in 1999 and now a Larsen & Toubro Group Company, Mindtree applies its deep domain knowledge to 350+ enterprise client engagements to break down silos, make sense of digital complexity and bring new initiatives to market faster. We enable IT to move at the speed of business, leveraging emerging technologies and the efficiencies of Continuous Delivery to spur business innovation. Operating in more than 15 countries across the world, we're consistently regarded as one of the best places to work, embodied every day by our winning culture made up of 21,000 entrepreneurial, collaborative and dedicated "Mindtree Minds."