Operationalize CCPA Compliance

CENTRL

White Paper

Table of Contents

Overview:
What you Need to Know About the California Consumer Privacy Act

Companies are confronted with a new and urgent challenge: how to comply with California's brand-new privacy regulation and provide greater control and transparency to customers over their personal data. The California Consumer Privacy Act (CCPA) offers consumers the right to opt out of the sale of their personal information, the right to access their personal information, and the right to delete their personal information. Although it doesn't apply to at least some small businesses, it is estimated that more than half a million businesses in the United States will need to provide these rights to California consumers. With enforcement starting in July 2020, the impetus for updating or creating a privacy compliance program should be at the top of major corporate IT initiatives for 2020 and beyond.

The CCPA introduces the following rights for consumers regarding their personal data:

- Right to know all personal data collected by a business
- Right to say no to the sale of personal data
- Right to delete personal data
- Right to be informed of what categories of personal data will be collected prior to its collection, and to be informed of any changes to this collection
- Mandated opt-in before sale of children's information (under the age of 16)
- Right to know categories of third parties with whom personal data is shared
- Right to know categories of sources of information from whom personal data is acquired
- Right to know the business or commercial purpose of collecting personal information
- Private right of action when companies breach personal data

Penalties - Proposed fines of the CCPA

Under CCPA, fines are enforced by the Attorney General and can reach up to $7,500 per every violation (in the case of intentional violations). Non-intentional violations are subject to a $2,500 maximum fine).

Additionally, CCPA allows affected consumers to file individual or class action lawsuits against offending businesses. Damages would range between $100 and $750 per violation.

CCPA - Which organizations must comply?

Organizations impacted by the CCPA are defined in **Section 1798.140(6)(1)(A-C)** of the bill. You are obligated to comply with CCPA and have DSAR requirements if your organization meets this criteria.

if ANY of the following apply:	And the following is true:
$25M + in annual gross revenues	You are a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of your shareholders or other owners. Note: the regulation doesn't appear to apply to non-profit organizations, but the California Attorney General and/or state legislature will further clarify.
50K or more consumers, households or devices have personal information you buy, receive for commercial purposes, sell, or share for commercial purposes each year.	A firm that "does business" in California.
50% or more of your annual revenue is derived from selling consumers' personal information	You collect consumers' personal information, or someone collects it on your behalf. "Collect" means to buy, rent, gather, obtain, receive, or even access information, by any means, whether actively or passively, including by observing a consumer's behavior. You alone, or jointly with others, determine the purposes and means of the processing of consumers' personal information.

Where to Start - Plan of Attack

Preparing for the CCPA can seem overwhelming if you plan on attempting to tackle every issue at once, particularly if you have multiple programs that touch consumer data or complex processes for data storage, manipulation, sharing and selling. Add in external vendors to the mix, and the overall plan of attack can appear daunting. Breaking down each facet of the regulation's requirements is a good starting point. Then mapping out what line of business, product, and the owners of each is next in line. Early planning sessions should include business/product owners, so they have visibility into all process streams that touch data. And consider that privacy compliance crosses almost every department within a firm. Stakeholders will exist across the entire organization, including departments such as marketing, HR, accounting and customer service. Gathering department heads across a company will ensure that you have tighter alignment with tangible business goals instead of getting lost in the details of process flows. But first off, there are a few immediate updates to your privacy compliance program that you need to address.

Consumer Data Intake, Collecting Consumer Information, & Updating your Privacy Policy

If you collect personal information **from a consumer** you must provide	If you collect personal information **about a consumer** you must provide:	If you sell or disclose personal information **about consumers**, you must provide:
Categories of personal information your business has collected. Specific pieces of personal information your business has collected. Assurances that you honor deletion requirements.	Categories of personal information your business has collected. Specific pieces of personal information your business has collected. Categories of sources from which the personal information was collected. The business or commercial purpose for the collection. Categories of third parties with whom your business shares the personal information.	Categories of personal information you have collected about the consumer. Categories of personal information you have sold about the consumer. Categories of third parties to whom the personal information was sold (organized by category of personal information for each third party). Categories of personal information you disclosed about the consumer for a business purpose.

Communicating with your Customers

Under the CCPA, businesses must inform consumers at or before the point of collection as to the categories of personal information (PI) to be collected and the purposes for which the PI will be used. Additionally, the CCPA includes a specific right to opt-out of the sale of personal information.

To comply with the CCPA you will need to:

- Include a "Do Not Sell My Personal Information" link on your home page
- Set up a publicly accessible web page to allow consumers to opt out, without requiring them to create an account
- Offer at least two methods for submitting requests for disclosure, including at the minimum a toll-free number and a mechanism on your website
- Respond within 45 days to a verified request in an electronic, transferable format.

Preparing for CCPA - The 5 W's and H of Preparation

It was probably in your elementary school years that you were first taught about the "5 W's and H" (who, what, when where, why and how), when you were first introduced to an organized way of gathering information or problem solving. Those basic tenets of discovery fit perfectly with the questions you need to share with your team when launching or updating your data privacy compliance program. Let's examine each, as they pertain to the CCPA.

Where is the data?

In the world of information security, there's a popular saying, "you can't protect what you can't find." With GDPR, and now CCPA, that similar principle applies to protecting the privacy of personal information; you can't protect personal data it if you can't first find it. In order to protect personal data, you first have to determine where every person's data resides. Finding data in an organization has never been an easy task. It was hard when data was largely confined to relational databases, file shares, email and mainframe computers. The task of finding personally identifiable information (PII) becomes more difficult with the adoption of big data stores, SaaS, IaaS and all sorts of content systems spread across both the data center and cloud.

Companies should create a data inventory or data flow map to understand all the ways in which they may obtain personal information, the types of personal information they collect and share, the purposes for which they use it, the parties with whom they share it and why, how it is retained and secured, and their current data deletion practices.

Who do you share data with?

As illustrated above, the "where" data in today's distributed world of data storage, is crucial to meeting the CCPA's call to action. Working hand-in-hand with the question of where data is stored, comes the question of "who?" have you shared consumer data with. Tracking customer data is a somewhat easier task when that data resides in intra-company data systems; modern privacy compliance software should be able to locate that data and automate the update of that information on an ongoing basis. The task of finding who exactly has customer data becomes increasingly difficult when that data resides outside corporate systems. Data can be shared, sold, and resold a multitude of times downstream. Mapping your data inventory with partners is essential for privacy compliance. And implementing an easy and repeatable way to query for that information can take the pain out a data deletion request, as the 45-day deadline clock of the CCPA ticks down.

What Personal Data do you have?

To prepare for CCPA, you'll need to know which data in your organization is relevant to the categories of personal information laid out in the law. You'll need a solution that can help flag data relevant to the CCPA, with customizable categories. If your enterprise needs to sort and normalize data categories, you should begin a data classification project. Maybe your team already has a good system in place to classify data; if so, find a solution that can provide a system that can seamlessly integrate with those systems, including one that easily receives data imports as well as works well with ediscovery solutions, need-be.

When do you need to respond to a subject action request by?

The CCPA's current requirement for a business to respond to a consumer's verified request for information is within 45 days (subject to extension under limited circumstances). This small window of time to receive, triage, route to the proper owner(s) of the data and respond to the request has the makings of a data routing nightmare. An enterprise needs to have processes and a solution in place to not only handle the basics of subject access requests (intake and deletion), but implement a system that can automatically discern what types of data have been received, where it resides (internally or externally), what current law(s) apply to the type of data, and by when the deletion needs to occur by. Also, keep in mind that the CCPA currently calls for a "12 month look back" period, which requires companies to be able to provide information to consumers about information collected or disclosed in the immediately preceding 12 months. That means companies should be able to find and report on what consumer data exists, how it's been used, and if it's been sold to third parties.

Why are you requesting the data?

As covered above, under the CCPA, businesses must inform consumers at or before the point of collection as to the categories of personal information (PI) to be collected and the purposes for

which the PI will be used. Additionally, the CCPA includes a specific right to opt-out of the sale of personal information.

To adhere to the new regulation, it's important for a firm to put in place a data inventory and mapping process that will provide a clear view of what data it holds and how it is used within and without your organization. Lacking this insight, your organization may struggle to efficiently and properly respond to a consumer request for access or deletion of personal information. Armed with this precise knowledge, your organization will know what personal data it possesses, making it easier to respond to consumer requests. In addition, your organization can better track the full lifecycle of data, verify data security controls, and finally, determine whether you have the right to sell consumer data to third-party vendors per the type of data and specific rule of law, be it the GDPR, CCPA or any other emerging legislation.

When deletion requests arrive, make sure that they are quickly routed and assigned to the proper owner of the data, and that the request is acted upon quickly. Instead of asking contacts within your firm, as well as third-party partners, to answer the same questions over and over – via emails, internal chat platforms, ticketing software, and spreadsheets, leverage an automated system that creates a simple, repeatable, and trackable process to record information relevant to consumer data. Look for a system that allows you to use easily configurable out-of-the-box questionnaire templates to quickly route data subject requests to the correct contacts within/without your firm. The solution should also be flexible enough to grow with your firm, as different emerging privacy laws will undoubtedly require additional processes to be implemented.

How will you act upon DSARs?

Data subject action requests involve not only team members around your organization, but also all vendors and partners with whom you shared the personal information. If you have shared personal information with different internal teams and systems, you must be able to track back to the data stores sources and request that the personal information has been deleted.

If you disclose personal information to third parties, such as partners or vendors, you'll need to be able to send a deletion request quickly to all of the external parties who have received that information. When outlining a data privacy compliance plan, think about creating a streamlined data subject rights management process that leverages intelligent templates and is easy to use. Plan on implementing a system that will be able to manage request due dates and extensions per the regulation – in this case, the CCPA – but also future regulations. Being able to link to your data inventory to track down data, and quickly collaborate with data process owners is paramount to success. Finally, make sure you have visibility into your workflows to reveal patterns (and possible roadblocks) in subject access requests with standardized reports.

Conclusion

Preparing for the CCPA may seem overwhelming, but it doesn't have to be painful. But add in the prospect of additional state and federal privacy laws going live; implementing a privacy compliance program is now crucial. One clear message has emerged: just as the European Union amplified and addressed consumer privacy rights in 2018 with the GDPR, the same has happened in the US. With 40 million residents, California is forging ahead to drive consumer privacy rights within the state, as well as with any business across the nation that does business in California. Companies will be required to have a clear understanding of the personal information they collect, process, use and share to be able to comply with the incoming law. The importance of building a data privacy compliance program now will help prepare businesses to meet this new and future regulations.

Appendix

Privacy Compliance Project Plan –Suggested Milestones

STEP 1:	STEP 2:	STEP 3:
Building the Team: Sync key stakeholders from across various departments	Data Analysis & Inventory	Maintenance of Ongoing Compliance Program
Product management Legal Information security Engineering Procurement Human resources Marketing	Privacy Risk Assessment Gap Analysis Communicate Risk Assessment and Gap Analysis findings to team Process Plan Formalize CCPA program team and roles/ responsibilities Set short, medium, and long-term objectives and success goals of the CCPA program Create Your Privacy Policy Program Launch	Annual Activities Review of policies Review and updating of personal data inventory Recurring privacy training Privacy program audits Data governance Individual privacy rights management; update as required Vendor risk management; update as required Continuous monitoring of privacy KPIs Communicate compliance initiative outcomes and future updates to departmental key stakeholders and executive team

CCPA Compliance Solution Checklist

When evaluating data privacy platforms, look for a flexible and robust solution that will allow:

Data Mapping & Data Inventory

- Implement an automated solution for mapping privacy data and input/output flows for CCPA, and future privacy regulations.
- Harvest questionnaire responses to automatically populate data inventory or use data discovery tools to get granular data elements.
- Provide a consolidated view of all processing activities, including the list of processors, sub processors, and data locations.
- View reports by data subjects and other attributes including cross-border transfers.

Data Subject Access Requests

- Implement a streamlined data subject rights management process with intelligent templates and simple user-friendly design.
- Manage request due dates and extensions per the regulation – CCPA, and future regulations
- Link to your data inventory to track down data, and quickly collaborate with data process owners.
- Embed branded request forms on your website, or inside of your product.
- Gain visibility into your workflows and reveal patterns in requests with standardized reports.

Readiness and Impact Assessments

- Conduct risk and readiness assessments to determine the handling of personal data.
- Evaluate responses, segment processes, and entities into tiers based on risk.
- Select high-risk processes and entities for Privacy Risk Assessments (PIA) and Data Protection Impact Assessments (DPIA).
- Conduct privacy audits and assessments on internal departments or external third parties.
- Track progress of each assessment and monitor associated risk in different risk categories.

Risk and Issue Mitigation

- Identify and raise the visibility of issues from each privacy assessment as well as third party or partner engagement.
- Collaborate with internal groups and third parties; request updates on issue remediation.
- Capture important details about specific issue severity, resolution recommendations, and issue status.
- Create action plans and manage progress from start to completion.

Reporting and Analytics

- Deliver comprehensive data mapping reports by data subject, processing activity, and other attributes.
- Track risk, status, and progress for each processing activity with the ability to drill down to the details of each process.
- Advanced search to quickly and easily find relevant items.
- Leverage portfolio-level dashboard and reports to highlight risks and exceptions.

Resources

https://iapp.org/news/a/top-five-operational-impacts-of-cacpa-part-1-determining-if-youre-a-business-collecting-or-selling-consumers-personal-information/
https://www.caprivacy.org/
https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/
https://www.fenwick.com/publications/pages/ccpa-vs-gdpr-10-things-to-do-now-to-prepare-for-the-strictest-us-privacy-law.aspx
http://en.finance.sia-partners.com/20180115/preparing-gdpr-why-you-need-ps15m-or-ps300-ps450-employee-average-implement-gdpr
https://iapp.org/news/a/top-5-operational-impacts-of-cacpa-part-3-responding-to-consumers-personal-information-access-requests/
https://iapp.org/news/a/top-5-operational-impacts-of-cacpa-part-2-transparency-and-notice-obligations/
https://www.exonar.com/the-impact-of-privacy-on-the-public-sector/
https://ico.org.uk/about-the-ico/news-and-events/blog-don-t-get-caught-out-by-subject-access-requests/
https://www.lexology.com/library/detail.aspx?g=39e38cc6-b7cf-4b3f-93d7-9ca16395f55d
https://www.grantthornton.com/library/articles/technology/2019/data-privacy-matters.aspx
https://iapp.org/news/a/where-to-begin-to-operationalize-ccpa-compliance/
https://www.dataprivacymonitor.com/ccpa/the-california-consumer-privacy-act-frequently-asked-questions/

Published: July 2019. Updated: January 2020.

v0120a