PACIFIC **D**ATA **I**NTEGRATORS

The California Consumer Protection Act

A Comprehensive Guide

Table of Contents

Executive Summary

The California Consumer Protection Act (CCPA) was signed into law on June 28, 2018, by California Governor Jerry Brown. This regulation will go into effect on January 1, 2020 and be adopted by the attorney general on or before July 1, 2020.

The CCPA applies to all for-profit companies that meet certain requirements (Page 3) and do business with California residents. Regardless of where a company is located—from Georgia to Maine, from Greenland to Mexico—if a corporation does business with California residents and meets the specified requirements, then it must become CCPA compliant. No exceptions.

When the CCPA goes into effect, it will grant California consumers many rights, allowing consumers to access the data collected about them and limiting what companies are legally permitted to do with customer data.

In the past, companies faced few regulations regarding customer data. In fact, only the recent General Data Protection Regulation (GDPR) in the European Union compares to the CCPA. Consequently, companies will have to make a lot of changes to grant these new rights to customers and will need to upgrade their approach to handling customer data in order to become CCPA compliant by the January 1, 2020 deadline.

Although it will be necessary for companies to make changes, not all of these changes will be restrictive. If anything, companies will be able to use this regulation as an opportunity to improve their data quality, governance, privacy, and security processes. Accurate, well-managed data comes with a plethora of benefits, which will be outlined later in this white paper. These benefits allow companies to better target customers, to have smarter rebranding and marketing strategies, to make reliable business decisions based on reliable data, and to allay customers' concerns over the privacy of their data.

The changes that the CCPA demands may be the first of their kind in the United States, but they certainly won't be the last—in the United States and elsewhere. Other states have already begun the process of creating similar legislation, as have other countries around the world.

Background

General Information

Consumers are becoming increasingly concerned with the privacy of their data. They fear hackers stealing their information, and with it their identities, money, and sense of security. Individuals and governments have also begun asking why companies need so much personal information, what they do with the data, and how they protect it. Today's global shift towards privacy saw its first monumental acheivement in 2016, with the passing of the GDPR in the European Union.

The CCPA will require businesses to grant consumers many new rights, including the right to:

- Be made aware of all personal data that a company has collected about them for free, twice annually.

- Opt out of the sale of their personal data.

- Sue companies that lose their information due to security breaches.

- Request that all personal information be permanently and completely deleted, if a customer desires.

- Be treated no differently if they choose to exercise these new rights.

- Be made aware of what type of data is collected about them, before it is collected.

- Better protection of minors' data. Data on children (16 and under) cannot be sold without the minor's parent opting in to the sale of their personal data.

- Know what third parties will gain access to their personal data.

- Know how and why data is collected on them.

These rights will alter the relationship between companies and consumers, forcing companies to be more transparent about data collection.

To Whom is the CCPA Relevant?

CCPA applies to businesses that have customers in CA or does business in CA and satisifes one or more of the following thresholds:

1. Have over $25 million in annual gross revenue.

2. Have over 50,000 consumers' personal information for commercial purposes.

3. Earn over 50% of annual revenue from the sale of consumers'

personal information.

California's population of almost 40 million citizens makes up the fifth largest economy in the world. With today's online market, California businesses aren't the only ones doing business with California residents. Companies in other states and even other countries will find that they have California residents and must become compliant.

Even if companies don't have California residents as customers now, it may be in their best interest to become compliant. This ensures compliance in the event that they want to do business with Californians and must suddenly become compliant or face fines—or lose the business of that consumer.

An Extra Challenge

The CCPA requires companies to provide a 12-month look-back on consumers' personal data upon a customer's request. This means companies must begin making changes immediately in order to become compliant by the 2020 deadline.

If a business waits too long to begin their CCPA compliance initiative,

they will find themselves unable to meet the requirements surrounding the 12-month look-back portion of the CCPA.

How Will the CCPA Benefit Businesses?

Data privacy is becoming more and more important to consumers. The CCPA is not the end of data regulation…it is merely a piece of the beginning. Becoming CCPA compliant is a big step, but it also prepares companies for the continued data privacy legislation that experts expect to see in the coming years. As new regulations are introduced, CCPA compliant companies will have a strong foundation of data governance upon which to build their compliance.

A more direct benefit is that of attracting consumers. Consumers value transparency and accountability. Companies that apply CCPA compliance across their enterprise rather than just with their California consumers will yield happier consumers. If companies must become CCPA compliant, they should apply the CCPA requirements to all of their consumers and reap the benefits of consumers who are happy with the data privacy provided to them. This is an opportunity to boost corporate reputation, if leveraged correctly.

And, of course, there are the obvious benefits of not having to face the threats of fines and lawsuits that non-compliant companies will face after the January 2020 deadline.

How to Make Compliance an Easier Journey

Enterprise Data Catalog

You cannot govern or protect data if you do not know that the data exists, or where it is held. This makes step one of any compliance, privacy, or security program simple—discover and understand your relevant data.

Discovering a company's data is an enormous challenge, due to the rise of cloud, big data, hybrid environments, and more. Even before this explosion of information, data siloes were enough to keep information hidden.

The CCPA applies to all customer data, everywhere. If a company has not taken the time to discover all their relevant data, then customer information may be left ungoverned simply because a corporation did not know it existed.

The solution to this is an enterprise data catalog. Informatica's Enterprise Data Catalog (EDC) is a powerful tool that scans a company's data to determine what data exists, where it resides, its quality, the processes that it touches, the stakeholders in charge of the information, where the data originated, and more.

Data stewards may think they can uncover these answers manually, and perhaps once upon a time they could. However, the sheer volume of information that flows through a modern enterprise demands a tool that can catalog data at a large scale.

Manual efforts cannot discover, map, or track an entire enterprise's information flow. EDC leverages the power of artificial intelligence and machine learning, providing visiblity into all data, wherever it resides.

This is why EDC is the best tool to help companies become compliant. Informatica has taken a monumental–and error prone–manual effort and replaced it with a robust, intelligent tool.

Only after EDC shows you your data can you begin to manage it.

Data Governance

Data governance is a framework used in the management of an enterprise's data assets. Data governance holds data to a certain standard, ensures key stakeholders have visibility into the quality of their data sets, and is essential to implementing and reporting on data privacy regulations. Data governance tools are becoming increasingly important assets to businesses, considering how vital data is to maintaining a thriving enterprise. However, with the CCPA and other regulations, data governance has become even more vital.

Historically, companies have had no choice but to manage data governance on spreadsheets or SharePoint. However, this method gives no insights into the quality of managed data, is tedious and time-consuming, and is constantly out of date.

The CCPA will require more from businesses in regard to the consumer data they hold. With a solid data governance infrastructure in place, corporations can better fufill the requirements of the CCPA, have greater visibility into the flow of their customer data, and more.

Companies that invest in data governance platforms reap many benefits of well-managed data, from compliance to more accurate business decisions. There is a reason that the AXON data governance platform is Informatica's fastest growing product in the history of their company. Simply put, data governance has a proven ROI.

"Data governance is a powerful tool with proven ROI and . . . is most effective when a data quality platform is already in place."

Since AXON is a scalable data governance tool, companies can start small and then scale their governance programs. For companies that are new to data governance, becoming CCPA compliant is a great first project. While companies may want to focus on other data-driven projects in the future, the CCPA provides a bite-sized starting point for implementing a data governance program.

After the CCPA is used to prove the ROI of data governance, data governance can be expanded to other projects and departments, and gradually expand its reach until the company has true enterprise data governance.

Data Quality

While data governance is the more obvious component of compliance, most data experts agree that data quality is the best place to start for companies that want to digitally transform how they handle data, customer data included.

It is difficult to govern inaccurate data, and even when it is governed, business analysts will not trust the data enough to leverage it. Having high-quality data makes the effort of data governance worth the investment because the data will be trusted by analysts, and the resulting business decisions will be trusted by executives.

It is also difficult to secure a company's sensitive information when the business is unsure where all of its sensitive information resides.

It is for these reasons that data quality is an important factor in becoming CCPA compliant. In fact, when data quality and governance are integrated as Informatica Data Quality and AXON can be, data quality helps data governance run more smoothly and more efficiently.

While Informatica Data Quality works to match and deduplicate data, resolving errors in company databases, AXON allows data stakeholders to see the data quality as information moves from system to system. Companies can see where there are drops in data quality and determine where data quality needs to be improved.

To summarize, data governance is a powerful tool with proven ROI and can be leveraged on its own, but data governance is most effective when a data quality platform is already in place. Having these tools in place will allow companies to shift more smoothly to CCPA compliance.

Entry Point Questions

Entry Point Question 1

How do I acquire sound data in order to launch more effective marketing campaigns?

After asking consumers for data (name, phone number, email, occupation, etc.) the most important step is how that data is treated. Having a data quality platform is the best way to ensure that data is organized well and duplicates are resolved if a consumer enters their information more than once. Clean, accurate, and organized data is possible through data quality platforms. That data can then by analyzed by business strategists and marketers. The key point is that the data a company has is reliable enough foundation of data on which to build smart strategies.

Entry Point Question 2

What precautions can I take to prevent having consumer data stolen?

Improving data quality is the best place to start when trying to achieve better data security. Data that is low quality can trigger false alerts, distracting companies from bigger problems or wasting their time. In some cases, this can also lead companies to lose trust in their security systems and fail to check on real threats under the premise that the alert is just another false alarm. Having high quality data allows companies to escape these "boy who cried wolf" situations.

Additionally, high quality data allows for important, sensitive data to be encrypted. Data that is mislabeled may not be given the level of security it needs, leading to at-risk, unprotected data. Companies should consider investing in a data quality platform in order to prevent these compromising situations.

Entry Point Question 3

Achieving a 12-month look-back is a tedious process. How can this process be simplified for my data managers?

There are data governance platforms available that help companies organize their data for easier access. Companies that invest in top-tier data governance programs will find that their process of supplying a 12-month look-back is much more feasible than it would be otherwise.

Companies that couple their data governance platform with high-quality data will be most efficient in becoming compliant with this regulation requirement. Data governance is complimented by data quality because data governance programs can better decipher where data is supposed to go when that data is of a high quality. Organization is key to achieving a 12-month look-back; data governance and data quality make that more manageable.

Conclusion

The CCPA will necessitate a shift for companies and how they handle consumers' personal data. Such a shift must begin to take place immediately if companies are to be compliant by their deadline. Time is running out to become CCPA compliant. Despite the pressure of compliance, companies should see the CCPA as a good thing—as an opportunity to improve and profit. After all, the CCPA will benefit companies in the long run by repairing trust with consumers.

Disclaimer

CCPA compliance approaches are not one size fits all. This document is meant to provide points that may be useful to consider in a business's CCPA compliance efforts and is not meant as legal advice, guidance, or recommendations. Businesses should seek their own legal counsel in realizing what requirements they must meet.

About Informatica

Informatica is the only Enterprise Cloud Data Management leader that accelerates data-driven digital transformation. Informatica enables companies to unleash the power of data to become more agile, realize new growth opportunities, and lead to new inventions resulting in intelligent market disruptions. With over 7,000 customers worldwide, Informatica is the trusted leader in Enterprise Cloud Data Management.

For more information, call +1 650-385-5000 (1-800-653-3871 in the U.S.), or visit www.informatica.com. Connect with Informatica on LinkedIn, Twitter, and Facebook.

About Pacific Data Integrators

Pacific Data Integrators (PDI) is an Informatica partner with a strong emphasis in the utility industry. For more information about our MDM solution, call +1 800-403-5213, or visit pacificdataintegrators.com. You can also connect with PDI via LinkedIn, Twitter, and Facebook.