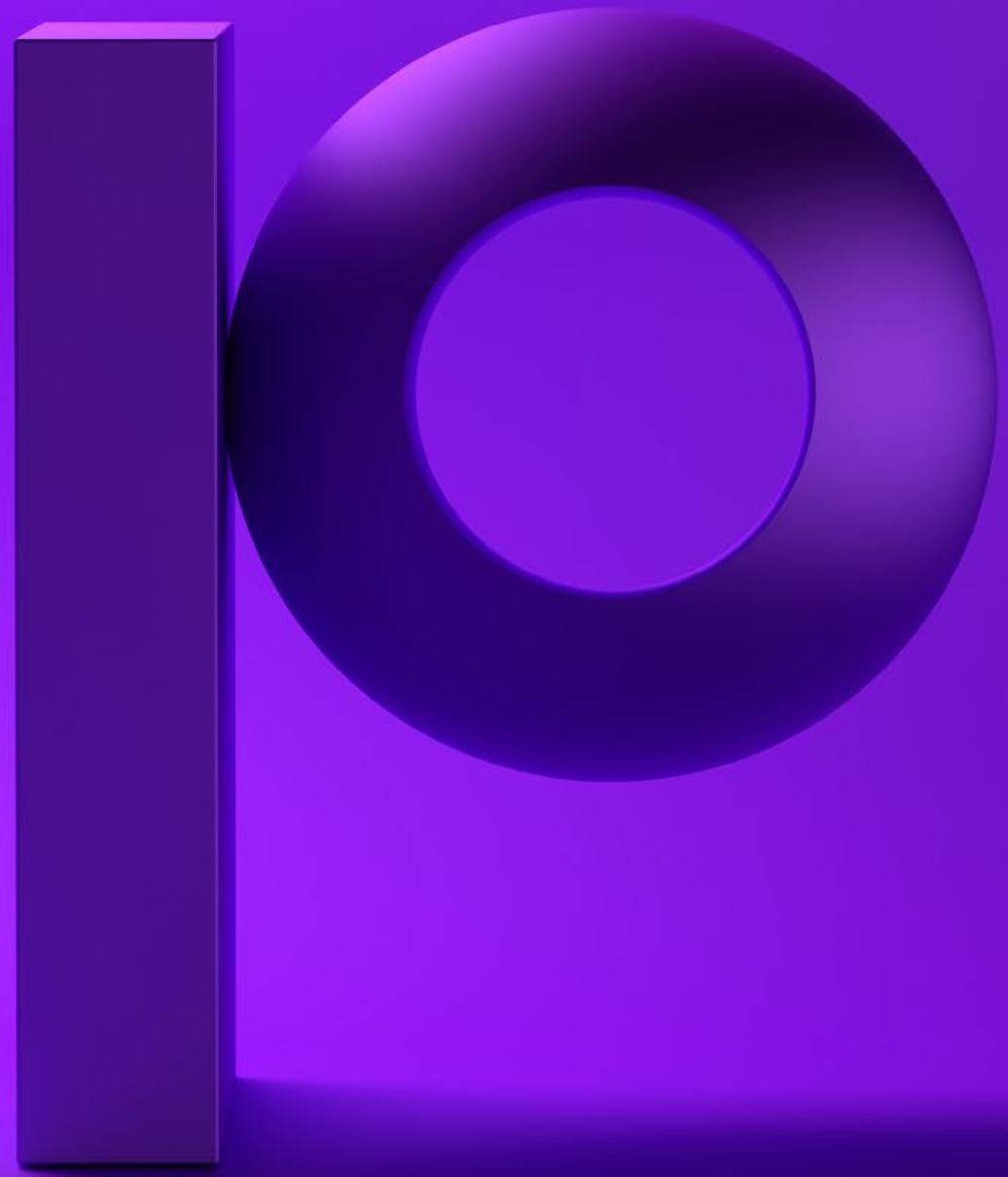
precisely

Data Governance Strategies for Addressing CCPA Requirements



Introduction

January 1, 2020, marks the start of not only a new decade, but also a new set of data governance challenges that will impact companies around the world. The California Consumer Privacy Act, or CCPA, which goes into effect on the first of the new year, imposes significant additional requirements to the ways in which companies manage data related to the consumers with whom they interact.

Although the CCPA is broadly similar in many respects to previous compliance frameworks such as the General Data Protection Regulation (GDPR), it creates some unique challenges that will require many companies to adapt their data governance and data privacy strategies.

And because the CCPA impacts not just companies based in California, but those that interact in any way with consumers who reside in the state, it has implications for organizations across the United States and beyond.

For these reasons, now is the time to begin planning for CCPA compliance, if your company has not already. To help with the process, Syncsort has prepared this white paper, which summarizes the CCPA's key data privacy requirements and explains how they compare to the mandates of the GDPR.

While the following pages do not address CCPA compliance strategies in exhaustive detail, they offer a concise overview of the key data governance practices that enable companies to successfully adapt to CCPA requirements -- as well as those of similar compliance frameworks that are likely to be passed in coming years by other U.S. state governments.

Core CCPA requirements

Designed to strengthen data privacy protections for consumers, the CCPA was passed by the California state legislature in June 2018, and its requirements go into effect on January 1, 2020.

Those requirements center around key aspects of personal data that companies collect or store:

- **Access**: Organizations must know about and provide consumers with access to any personal data that organizations collect about them. They must also consider all replicated copies, including reports and spreadsheets.
- **Transparency**: Consumers must be notified of any personal data that organizations are collecting about them. Therefore, organizations must have accurate and current addresses and email information for notification purposes.
- **Deletion**: Organizations must delete personal data that they maintain about individual consumers upon request.
- **Sales**: Consumers have the right, upon request, to prevent companies from selling their personal data. This means organizations must have the ability to flag content and have content connected to flag locations. They must also validate that flags are populated.

The CCPA contains an expansive definition of personal data, which it defines not just as data that directly relates to or describes an individual, but also any data that could potentially be associated with or indirectly linked to an individual or a group of individuals within the same household. Organizations that have not captured household identifiers before must do so now and commit to maintaining them. They must also apply data matching tools to identify households.

Thus, it is not only entries within a database containing an individual's name and address that are governed by CCPA requirements. Any data instance with any type of information that could potentially be personally identifiable — from a phone number and email address to an IP address, mobile device, and Web browsing history — must be governed in a way that ensures CCPA compliance.

Even data that has ostensibly been anonymized to some degree (by, for example, stripping it of personal names) could potentially be subject to CCPA requirements if it contains other types of identifiers that could be linked in some way to an individual or a household.

The CCPA also impacts data that is "scattered" across multiple databases but could potentially be linked together in a personally identifiable way. For this reason, distributing personal information across different databases is not sufficient for avoiding CCPA requirements (and, as this white paper explains below, identifying relationships between scattered data is critical for ensuring CCPA compliance).

Also important for companies to understand is that the CCPA applies to data collected about any resident of the state of California, regardless of where the company that collects or stores the data is based. As long as a company is doing business in California (even if just hosting a website that is available to California residents), the CCPA's rules apply.

For this reason, the CCPA bears important implications for companies around the world. Most companies with a digital presence have no practical way of avoiding engagement with consumers from California, and will, therefore, need to prepare for CCPA requirements.

What's more, about twenty other U.S. states have draft regulations similar to the CCPA under consideration or already ratified by legislatures. Thus, even if the CCPA itself truly does not apply to your company because it does not do business with consumers or operate in California, there is a high likelihood that other states' equivalent laws will impact your organization within the next few years. Preparing for the CCPA will help companies meet the requirements of similar frameworks enacted by other states.

CCPA vs. GDPR

The CCPA is comparable in many ways to the GDPR, a data privacy framework created by the European Union that took effect in May 2018. Both frameworks require companies to take reasonable measures to ensure the privacy and security of data that they collect.

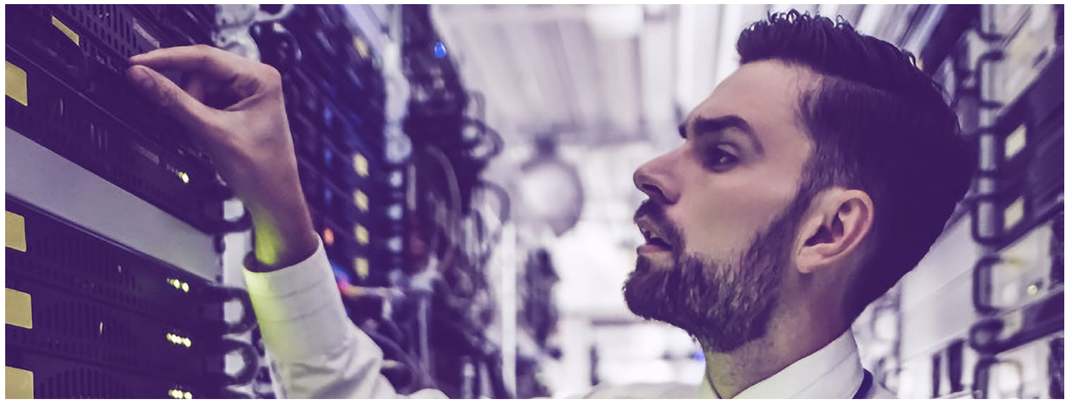
Both are also similar in that they do not define specific tools or practices that are required to meet their mandates; instead, they leave it up to organizations to determine how best to satisfy their requirements.

However, the CCPA and GDPR differ in many of their details. The CCPA applies only to companies of certain sizes and types — specifically, those that generate annual revenues exceeding 25 million dollars, maintain at least 50,000 instances of personal information or earn half of their revenue from selling personal information. In contrast, the GDPR applies to any company that collects and/or stores personal data.

The CCPA is also different from the GDPR in that the former has a more expansive definition of personal data. As noted above, not only personal names but any type of data that could potentially be linked to a person or a household, such as a phone number or even data about an individual's educational history, is defined as personal data under the CCPA.

A third major difference between the CCPA and the GDPR is that the CCPA requires companies to give consumers an explicit opportunity to opt-out of the sale of their personal data. The GDPR does not impose this requirement.

Because of these differences, the strategies that companies have developed over the past several years for GDPR compliance are probably not sufficient for achieving CCPA compliance as well. The CCPA requires some different tools and strategies.



Data Governance Strategies for CCPA

Effective data governance is the key to CCPA compliance. Data security is a consideration as well, but because the core compliance challenges of the CCPA involve finding and managing personal data in ways that meet regulatory requirements, data governance lays the foundation for meeting CCPA challenges.

The following are four key data governance practices that organizations must follow in order to satisfy CCPA mandates.

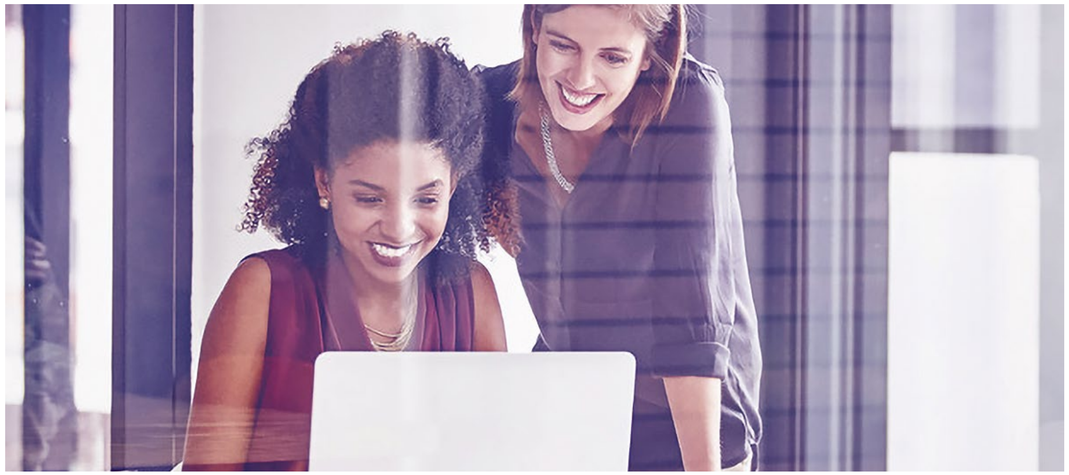
1. Finding relevant data

The essential first step for CCPA compliance is identifying which data your company collects or stores that is subject to CCPA requirements. It's only by knowing where relevant data exists that organizations can meet the opt-out and disclosure requirements of the CCPA, as well as delete consumers' personal data upon request.

Organizations can do this by profiling the data that they process and store — which means assessing its structure and content, and the relationships within it and connected to it — in order to determine where CCPA-relevant data resides. In most cases, data profiling is a more effective and accurate way to find relevant data than an approach that relies on metadata or data catalogs.

First, the latter resources are effective only if they were created with the goal of flagging the types of data that the CCPA defines as personal data. This is unlikely to be the case, given that many types of data that would not conventionally have been defined as personal data are treated as such under the CCPA.

Second, these resources can be cryptic and may not accurately reflect the actual data content. Because data profiling provides insight into data at its source, it is a better method of finding CCPA-relevant data than are more abstract representations of the data.



2. Managing and matching scattered data

Because of the CCPA's expansive definition of personal data, companies are likely to find that much of the data that the CCPA protects is spread across multiple databases. For example, an entry in a payment-processing database might be linked to another entry for the same customer in a customer master database. The CCPA would require both data instances to be treated as personal data, even though they are different types of data and are stored in different databases.

To address this challenge, organizations likely need a two-fold process. First, they can utilize the join (or cross-table) analysis techniques within data profiling to identify common keys (including data such as national identifiers, IP addresses, and phone numbers) that can identify relationships between data sources, regardless of where the data is stored. Second, they can deploy data matching tools to find and link data without common keys such as names and addresses. These tools leverage a broad array of matching algorithms to address issues such as spelling variations, mis-keyed data, and missing pieces of data.

By pairing data profiling and data matching techniques, businesses maximize their ability to identify CCPA-relevant data, even if the data is stored in formats or locations that they cannot predict ahead of time.

3. Continuous data monitoring

Data profiling and data matching can help to identify CCPA-relevant data at a given point in time, and therefore help organizations understand where relevant data is located and how to manage it. However, knowing where relevant data exists on a certain hour, day or month is not enough. Businesses must also monitor data on a continuous basis.

Continuous monitoring through ongoing business rule validation is the only way to achieve a quick notification in the event that your business begins storing personal data in a location not previously intended for that purpose, or if a new data pipeline or integration with a third-party data source creates implications for CCPA compliance.

To support CCPA compliance, data sources must be configured with data flags that continuous monitoring tools can recognize in order to assess whether a given database or data instance is impacted by the CCPA. Flags must have the ability to be customized, and new flags added, in order to support changing databases, data systems, and so on. Flags are also needed to test and confirm opt-out requirements. As an ongoing operational process, business rules applying data quality checks must be evaluated and updated regularly to ensure effectiveness.

4. Empowering data stewards

Finally, companies must take steps to ensure that the staff members who bear primary responsibility for managing data are empowered with the tools and processes they need to meet CCPA challenges.

Maintaining a data catalog and data profiling results is required to ensure that data stewards can understand their data and identify issues. Equally important is having the data monitoring and data quality processes in place that will generate alerts when compliance flags are triggered.

And when alerts happen, data stewards must have a process in place for determining who will respond, how information will be shared during the response process and how the incident will be communicated to stakeholders (possibly including the consumer) to ensure that the issue does
not recur.

Summary

Even for businesses that have excelled at meeting the requirements of the GDPR and other compliance frameworks, the CCPA introduces a set of additional compliance challenges that require new data governance tools and strategies.

Because the CCPA, along with similar regulatory frameworks that are poised to be applied by other states, will impact countries across the globe, it is crucial for organizations to adopt the solutions they need to find, connect, monitor and manage the many types of data that the CCPA protects.

Precisely Trillium for Data Governance can help. By delivering the data profiling and data quality processes that enable effective data governance and integrating those results to data governance and reporting tools, Syncsort Trillium empowers organizations to collect, manage and monitor data in ways that meet CCPA compliance requirements.

Learn more from the Precisely Trillium for Data Governance solution sheet.

precisely

Precisely is a global leader in data integrity, providing accuracy and consistency in data for 12,000 customers in more than 100 countries, including 90 percent of the Fortune 100. Precisely enables companies to integrate, verify, locate, and enrich their data to power better business decisions. To learn more, visit www.precisely.com.

www.precisely.com