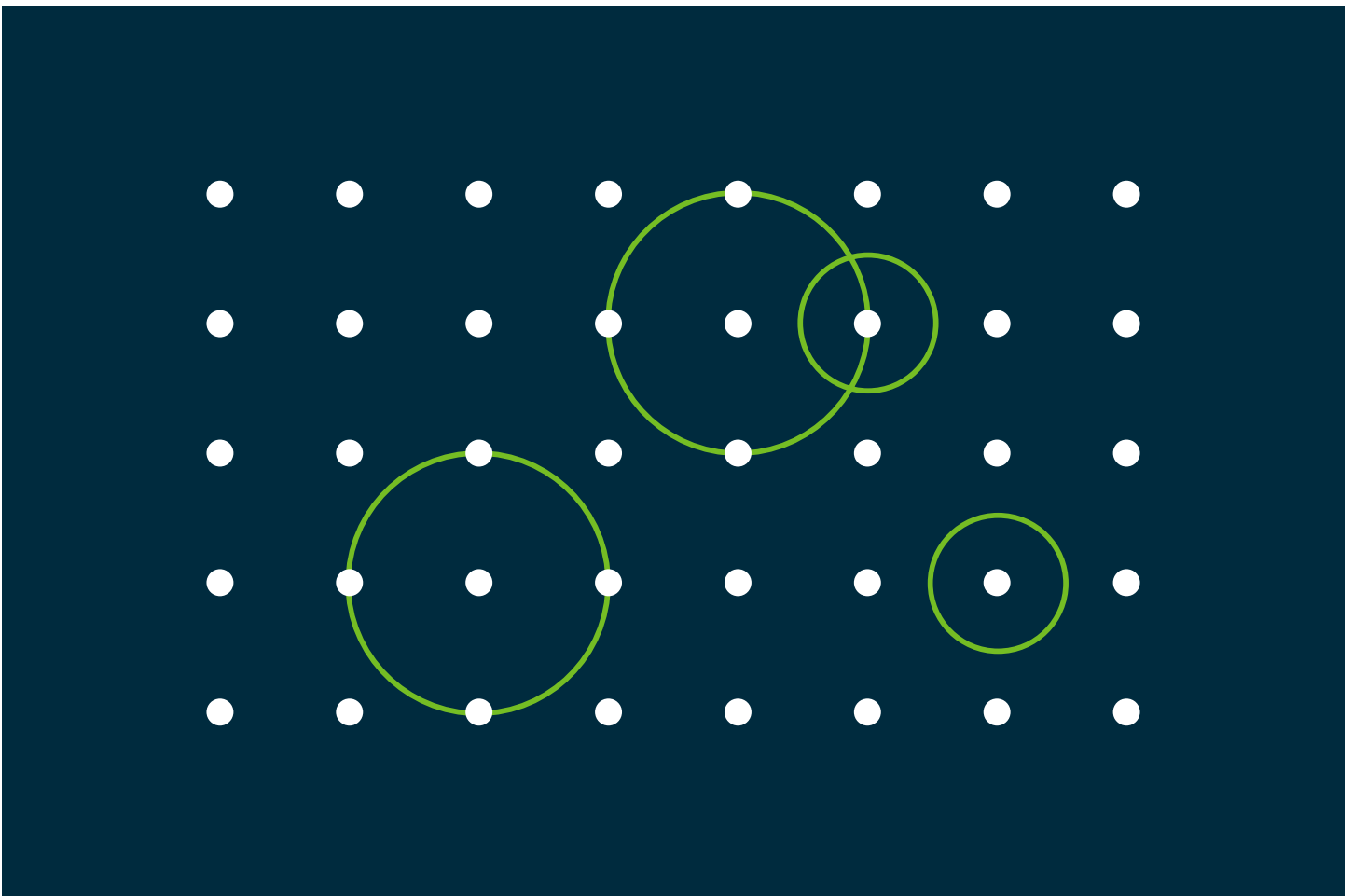


A guide to consumer rights request management

Putting data at the center of your CCPA strategy



Introduction

Consumer rights management is going to be a hot topic over the next few years. Attitudes towards data privacy are evolving, new legislation will take hold across more jurisdictions, and heavy penalties for non-compliance will come into force.

94%

of CEOs consider customer and client preference data as critical to business strategies

- PwC's 22nd Annual Global CEO Survey

The growing tendency for consumers to exercise rights over their data stems from two overarching trends:

1. The value of consumers' data is increasing

As more firms undergo digital transformation, they seek to collect more data and use it more intensely. They may analyze consumers' data to understand buying preferences, including brand affinities and price sensitivity. They may feed the data into the development of new products and services. In some cases, the data itself becomes the product.

2. Consumers' attitudes towards data privacy will continue to vary

Not everyone agrees with how their data can be used. Some happily consent to companies using their data to improve offerings, while others see such use as an invasion of privacy. Attitudes also change as new technologies emerge and in light of new information and circumstances.

Understanding these two trends helps explain why consumer rights management will only grow in prominence. Organizations are looking to do more with consumers' data and extract greater value from its use. Not all consumers agree with organizations' practices and some would rather opt out. As such, organizations are increasingly under pressure to respond to consumers exercising their expanded privacy rights.

Some organizations have responded by deploying point solutions that focus only on supporting the interaction between the requestor (consumer) and respondent (organization). However, such an approach represents a short-term tactical response to an overarching trend.

Over time, organizations need to take a more strategic approach to the challenge - focusing on the way to access and utilize their existing data infrastructures to support consumer rights requests and additional privacy use cases. Taking a data-centric stance enables companies to respond faster and with more confidence to the California Consumer Protection Act's (CCPA's) consumer rights requirements and future regulatory obligations.

Taking a data-centric stance enables companies to respond faster and with more confidence to the California Consumer Protection Act's (CCPA's) consumer rights requirements and future regulatory obligations.

This paper will examine:

- Consumers' rights over their data, focusing on the CCPA
- Commonly faced challenges for supporting a data-centric approach to consumer rights requests
- Critical capabilities needed to address consumer rights requirements in a Data Intelligent manner

Consumer rights under the CCPA

The CCPA is specific in its scope – not only in terms of its consumer rights, but also who can exercise those rights, organizations required to comply with consumer rights requests, the classification of personal data, and conditions around complying with consumer rights requests. To clarify, while the CCPA uses the terminology 'consumer,' the General Data Protection Regulation (GDPR) refers to this similar group as 'data subjects.' The term 'consumer' will be used in this paper for clarity and consistency.

Consumers in scope

The CCPA applies only to consumers that are residents in California. It does not apply to those visiting California on a temporary basis, but continues to cover California residents that leave the state temporarily.




Given that the CCPA is consumer focused, it would be simple to assume that the act applies only to B2C operations. However, that is not the case. Consumers are afforded the same rights when submitting a rights request to a B2B organization.

Companies in scope

Companies that do 'business' in California are subject to the CCPA. 'Doing business in California' is a broad term that essentially covers any company collecting personal information (PI) relating to California residents. However, there are additional criteria that would exempt small businesses. To be in scope, organizations need to have at least \$25 million in annual revenue, handle personal information from more than 50,000 consumers, or generate more than 50% of annual revenue from selling personal information.

Who must comply

A business will need to comply with CCPA if it is a for profit entity that...

 <p>Does business in California</p>	 <p>Collects PI or has it collected by others</p>	 <p>Determines purposes of processing PI <i>solely or jointly</i></p>
-----------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------

AND meets one or more of these criteria:

<p>50% or more</p> <p>Earns 50% or more of its annual revenue from selling PI</p>	<p>50K or more</p> <p>Works with PI for 50,000 or more consumers, households or devices</p>	<p>\$25 million+</p> <p>Annual gross revenue is \$25 million or greater</p>
----------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------

Definition of personal information

Under the CCPA, the definition of ‘personal information’ includes any information that could be associated with a particular consumer or household, either directly or indirectly. The legislative text specifies a number of examples of personal information, although declares that these are not exclusive.

Examples include typical identifiers such as names, aliases, postal addresses, unique personal and online identifiers, IP addresses, email addresses, and social security, driver’s license and passport numbers. They also include biometric information, geolocation data, commercial information and internet activity.

“Personal information’ means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”

- TITLE 1.81.5. California Consumer Privacy Act [1798.100 - 1798.199]

Description of Rights

The rights afforded to consumers under the CCPA can broadly be grouped into the following categories:

- **Right to be informed.** This includes both “the right of Californians to know what personal information is being collected about them” as well as the right “to know whether their personal information is sold or disclosed and to whom.”
- **Right to opt out.** This refers specifically to having information sold, enabling Californians “to say no to the sale of personal information.” It does not necessarily restrict other forms of information processing.
- **Right of deletion.** This allows consumers the right to request that their personal information be erased. However, it is subject to a number of conditions; for example, companies can still keep information to protect against fraud or to comply with other legal obligations.
- **Right of access.** This includes the right for consumers to obtain “the specific pieces of personal information” that have been collected about them, along with the sources of that information, the purpose for collecting or selling that data, as well as third parties with which the information is shared.
- **Right to non-discrimination.** This right ensures that Californians can exercise rights over their data without fear of discrimination. Specifically, the regulations guarantee “the right of Californians to equal service and price, even if they exercise their privacy rights.”

Responding to consumer rights requests

When a consumer looks to exercise their rights under the CCPA, organizations are required to respond within 45 days. PI will need to be provided “free of charge,” unless the business can show that such requests are “manifestly unfounded or excessive.” In some cases, the time to respond can be extended (by either 45 or 90 days depending on the complexity of the request), but only if an organization notifies the consumer of this prior to the initial 45-day period elapsing.

When responding to requests, organizations will have the choice of either providing information in writing or electronic format. If choosing the latter, the legislation states the “information shall be in a portable and, to the extent technically feasible, in a readily usable format that allows the consumer to transmit this information to another entity without hindrance.”

The 4 Rs of consumer rights request fulfillment

- 1 Receive
- 2 Review
- 3 Retrieve
- 4 Respond

Meeting all of these criteria means organizations will need to count on some key data workflows:

- **Receive.** Any new request that comes in will have to be logged, irrespective from which channel it comes. In many cases, the legislation specifies that organizations need to make at least two methods available for making requests – “at a minimum, a toll-free telephone number, and if the business maintains an internet website, a website address.”
- **Review.** Consumer rights under the CCPA are not absolute, so any inbound request will need to be reviewed to ascertain whether they meet all relevant criteria and can be carried out without prejudice to any of the organizations’ other legal obligations.
- **Retrieve.** Should the inbound request be approved, relevant information will need to be retrieved (in the case of information access requests). Equally, requests for information to be deleted or to opt out of sale, will need to be processed.
- **Respond.** Once the necessary processes are complete—either retrieval of personal information, deletion of it, or controls placed around its processing/sale—a response can be sent to the consumer to fulfil the request.

Complexities of data management for consumer rights

Solving data problems is hard, and organizations that approach data as an afterthought to addressing privacy use cases are likely to face a number of challenges. These challenges become even more complex when frontend-centric privacy solutions have already been adopted without a solid data foundation. Below are some of the most common impediments facing organizations:

Fragmented data and application architectures

Organizations have developed fragmented data and application architectures for a variety of reasons, not only as a result of mergers and acquisitions, but also through organic proliferation of new systems and processes. As such, simply identifying all source systems that store personal information is a challenge.

What the market says:

More than half of Data Privacy Officers (56%) state that the most difficult type of data subject requests involve locating unstructured personal data.

- IAPP-EY Annual Privacy Governance Report, 2019

“Adapting to an increasingly volatile regulatory environment is one of the top priorities for data and privacy professionals, but only 4 in 10 privacy executives are confident in their current abilities to keep pace with new requirements”

- Gartner, Discussions With Privacy Executives, 2019

Lack of insight into data flows

In order to efficiently manage these requests, teams need to know where personal information is stored, how it is processed and for what purposes; nonetheless, many organizations lack clarity about how data flows through their ecosystem. Organizations need an understanding of data lineage – how data flows through various systems and processes. While technical data lineage can be important to understand system dependencies, maintaining a high-level map of business lineage can help understand how different datasets flow through various business processes.

Lack of granular access controls

The right for consumers to restrict processing of their PI can prove problematic for organizations that are not able to control access to data on a granular level. Inaccurate categorization of both data and business processes complicates managing data access and permissions according to specific use cases.

Incomplete data governance

In addition to having the right systems in place to understand where personal information is stored, how it is processed, and how access can be controlled, it is vital to have the right people, policies and processes in place to ensure accountability and oversight. Unfortunately, many organizations do not have a foundation of data governance in place. Data governance is an enterprise responsibility; it is important to recognize that data governance and data privacy affect every team that uses data, including BI/analytics, finance, marketing, IT and more. Clarifying responsibilities for data and requirements for proper usage will help to coordinate responses to consumer rights requests.

Take a data-centric approach for consumer rights requests

It’s not enough to just know the ins and outs of privacy legislation. In order to efficiently manage consumer rights requests, organizations need to put data at the center of their privacy strategy. Organizations that implement a data-centric

approach must rely on several data competencies. From a high-level perspective, they need to be able to keep track of all sources of PI, understand how they are processed (and for what purpose), understand which policies apply to which datasets, and maintain granular controls to restrict certain processes.

Assessing these broad competencies in more specific terms, organizations will need the following capabilities:

PI discovery and classification

To prepare for the CCPA and respond to consumer requests, organizations need to know where their data is and what kind of data it is. Consequently, PI discovery and classification capabilities are indispensable for an effective consumer rights management program.

PI discovery helps organizations get visibility about where their data privacy and security efforts should be focused. This allows privacy teams to map out where PI is stored throughout the enterprise's data ecosystem. PI discovery is not an isolated task performed at the beginning of a privacy program; it is essential to scan data and give it context periodically. Therefore, investing in automatic PI discovery tools enables organizations to scale as the CCPA evolves and as new regulations emphasize consumer rights.

Once data is monitored, organizations must be able to categorize and systematize the data to use it compliantly and productively. Automatic PI classification enables organizations to populate data in a more scalable manner, ensuring new sources can be on-boarded into a catalog without undue amounts of manual effort.

Process register

Organizations are held accountable for knowing and communicating how and why they use data. A process register gives data context. It effectively maps out business processes associated with personal information so that an organization understands the purpose behind the processing of such information, the data categories in question and the legal bases under which this information is being processed. This helps to ascertain whether, for example, a request to have information deleted can be carried out in its entirety, or whether some information will need to be retained to comply with other obligations.

“Companies need to define the types of data collected and retained—and which data is personal versus public—in a manner that’s compliant with privacy regulations and that clearly classifies individuals impacted by the information to ensure customer access requests are properly addressed.”

- Deloitte, Data privacy as a strategic priority, 2019

Collibra for individual rights request management

By providing a foundation of Data Intelligence, Collibra Data Privacy enables organizations to accelerate and sustain compliance with the CCPA and manage consumer rights requests. Privacy by design is embedded into a single platform, allowing cross-functional teams to operationalize privacy. By offering a single platform and capabilities such as Intuitive Workflows, PI Discovery & Classification, Process Registers, Data Mapping, and Reporting & Dashboards, Collibra Data Privacy puts data at the center of privacy compliance programs. Collibra Data Privacy provides visibility and transparency into PI, increasing speed and accuracy of request responses.

Collibra Data Privacy ultimately facilitates consumer rights requests with the Individual Rights Request (IRR) management feature. Consumer requests require multiple stakeholders, including the privacy team to manage the request, data owners to extract or delete the data, and business owners to identify the initial business purpose for the collection and usage of the data.

Collibra’s IRR feature simplifies collaboration for consumer rights request fulfillment. IRR leverages the power of the Collibra Platform by streamlining collaboration with role-relevant context and notification and automating workflows in a centralized location. By bringing everyone to one platform built with Data Intelligence, Collibra covers the end-to-end process of consumer rights management: from registering a new request, to fulfilling the request, and to sending a final response to the consumer. Privacy teams can even respond to audits and reporting requests by documenting steps taken along the way

within the platform. With Collibra Data Privacy, organizations can put data at the center of a scalable privacy strategy and instill trust in their consumers.

Conclusion

The value of this data is growing at an unprecedented rate. We have yet to fully appreciate the ways in which this value can be realized, but we know data has the potential to revolutionize how organizations operate and go to market.

However, changing consumer preferences and regulations are complicating how organizations take advantage of data. Not everyone agrees with how their data can be monetized. Some are concerned by the volumes of data being collected and see this as an invasion of their privacy. In order to protect consumer rights, governments are affording consumers more control over their data and incorporating those rights into legislation.

From the perspective of the enterprise, the rights afforded to consumers over their data can pose significant challenges, but the enterprises can deploy technology and processes to protect their consumers and intensify operational efficiency. It is important that organizations take a data-centric approach to consumer rights. That means keeping an accurate map of where personal information is stored, how it is processed and for what purpose, as well as understanding which policies apply to which datasets and use cases. By taking an approach built on a data foundation, organizations can tackle consumer rights and retain trust, now and in the future.

Collibra is the Data Intelligence company. We accelerate trusted business outcomes by connecting the right data, insights and algorithms to all Data Citizens. Our cloud-based platform connects IT and the business to build a data-driven culture for the digital enterprise.

 **If you are interested in learning more, please visit our website and request a demo at collibra.com/request-a-demo**