TOKENEX


EBOOK

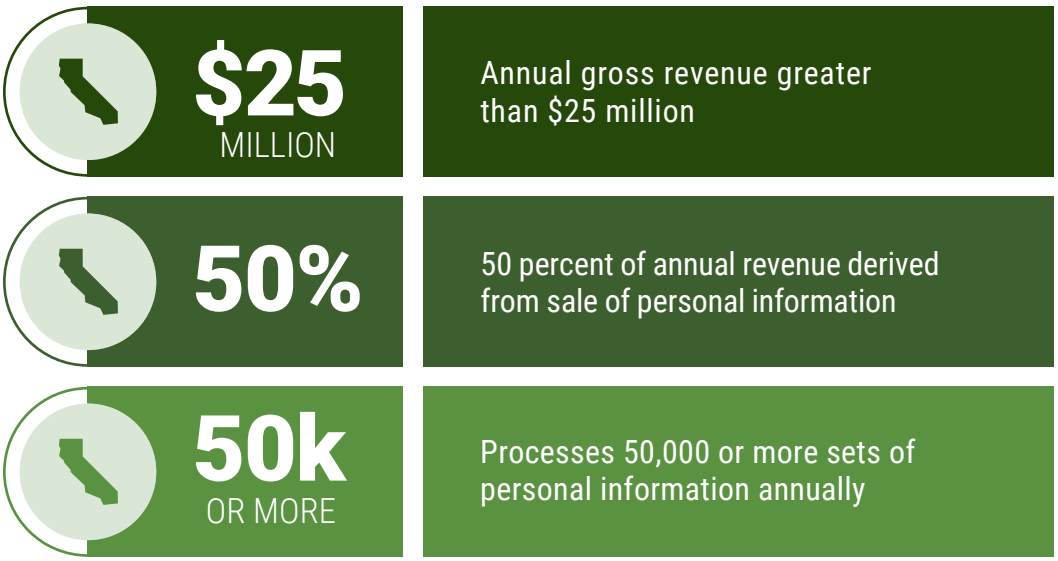
# CCPA COMPLIANCE GUIDE

How cloud tokenization and proper data collection practices can help you meet the data privacy requirements of CCPA

## SHAPING THE PRIVACY LANDSCAPE

The California Consumer Privacy Act ("CCPA") was enacted to protect the privacy of California citizens and households. The CCPA establishes requirements for the collection, processing, and sale of their personal data, as well as introduces measures that enable them to control how their personal information is stored and processed.

Similar to the European Union's General Data Protection Regulation, the CCPA's reach expands beyond its legislative boundaries. It applies to all businesses that collect the data of Californians and fall in a designated earnings bracket, derive at least half of their revenue from selling the personal data of California residents, or interact with the data of a certain number of Californians.




The CCPA is a response to a demand for stricter regulation, stronger penalties, and more thorough enforcement for businesses whose practices result in the mishandling and/or exploiting of their customers' personal data. The CCPA is often, and correctly, characterized as one of the first American attempts at comprehensive privacy regulation.

## WHAT YOU NEED TO KNOW

To better understand how the CCPA affects you and your business, this paper outlines the details, definitions, and penalties included in the CCPA. As the number of data privacy laws increases globally, it is important to know the risks of noncompliance as well as the technologies that exist to help simplify the compliance process by properly protecting personal data.

The CCPA likely will continue to be amended and influence the burgeoning privacy regulations in other states, just as the GDPR set the global standard for the collection, handling, and use of personal information. With this in mind, compliance should be seen as an ongoing evaluation of your organization's systems, processes, and practices to ensure your business is positioned to deal with future regulatory obligations as well as today's.


FOR A DETAILED EXPLANATION OF KEY TERMS AND CONCEPTS, **CLICK HERE** TO VIEW OUR GLOSSARY.

## WHY IT'S IMPORTANT

Although some might view the CCPA as an overreaction to the Cambridge Analytica scandal, the exposure of personal data through data breaches has become an all-too-common occurrence among even the most technologically savvy companies. The reality is that many organizations are not securing personal information properly because they have had no legal reason to do so.

Despite existing data protection measures such as the Payment Card Industry Data Security Standard (PCI DSS) and Gramm–Leach–Bliley Act (GLBA), there is no single, comprehensive U.S. law that covers the scope of the capture, storage, or use of personal data. Similarly, although the Federal Trade Commission is the de facto watchdog for data breaches, there is no single, central agency or body that has regulatory oversight of information and data security.

As more states pass regulations like the CCPA, the industry is likely to see additional efforts at comprehensive Federal legislation, in an effort to reduce the complexity of a privacy landscape that varies from state to state.

From a global perspective, many organizations that are already subject to GDPR will also be required to comply with the CCPA. Although those who already are compliant with the GDPR are not certain to be compliant with the CCPA, they will certainly be better prepared.

If your organization is already operating in compliance with the GDPR or you're familiar with the regulation's general requirements, check out our comparison to see what additional steps you'll need to take to comply with CCPA.

CLICK HERE TO VIEW OUR
**CCPA vs. GDPR** COMPARISON

## HOW TO COMPLY

CCPA compliance requirements can essentially be sorted into one of two categories. The first is concerned with the processes and technologies used by covered entities to manage the personal information they gather and possess. The second category consists of measures surrounding the security of that personal information, specifically the systems and standards in place to protect against data breaches, mitigate breach effects, and respond to a data breach in the event that one occurs.

Below, we'll cover specifics surrounding compliant practices for data collection, management, reporting, and response—emphasizing transparency and sound data-processing procedures. Additionally, we'll address proper data-protection techniques for reducing the potential risk and impact of breaches.

## IDENTIFY AND LOCATE CONSUMER DATA

The first step is to find the data you need to protect. Known as data discovery, this process will enable you to determine the extent of personal information you possess, how it's traveling through your environment, where it's being stored, and with whom it's being shared. You can use vendor-provided technologies and tools for data discovery and classification to help streamline this process of mapping the personal information throughout your environment.

Once data is discovered and documented, it is advisable to minimize storage areas and delete any data that does not provide immediate technical or business value. You'll also want to evaluate your data collection practices and ensure the data you're collecting, storing, and/or sharing is related to a sale, provision of a service, or another business purpose, as required by the CCPA. Additionally, if you've shared personal data with any third party, make sure that third party is properly using and protecting it.

## PUBLISH NOTICES DETAILING DATA COLLECTION PRACTICES

The CCPA also requires organizations to create—and make readily available—notices regarding the purposes and processes for personal information collection. These are generally known as privacy notices. This information must be disclosed before any protected data is collected.

Items that must be contained in the notice include the types of information collected, from where they are being collected, and with whom they are being shared. All of the preceding information should be publicly accessible and provided to consumers upon request. It should also be updated as changes to your processing practices occur.

**NOTICE AT COLLECTION**

THE CCPA ALSO REQUIRES ORGANIZATIONS TO CREATE–AND MAKE READILY AVAILABLE–NOTICES REGARDING THE PURPOSES AND PROCESSES FOR PERSONAL INFORMATION COLLECTION.

## INCLUDE OPT-OUT LINK ON WEBSITE

The home page of any covered entity's website must contain a prominent link that when clicked will give users the opportunity to opt out of data collection, sharing, or sale. This link must then direct to a page where individuals can revoke any previous consent to the sale of their personal information.

The link must be specifically titled **"Do Not Share My Information,"** and it cannot require account creation or be part of any other information-gathering process. If an organization wishes to request permission to sell the personal information of an individual who has previously opted out, it must wait at least 12 months before making that request.

## IMPLEMENT PROCESS FOR HANDLING CONSUMER REQUESTS

Organizations that receive a consumer request provided for by CCPA must respond and fulfill it within 45 days without requiring the consumer to pay a fee in order to satisfy the request. Because processes must be in place to meet these inquiries in a timely fashion, it's a good idea to make them a permanent, documented part of your internal information technology and security practices.

**"DO NOT SHARE MY INFORMATION"**
THE HOME PAGE OF ANY COVERED ENTITY'S WEBSITE MUST CONTAIN A PROMINENT LINK THAT GIVES USERS THE OPPORTUNITY TO OPT OUT OF DATA COLLECTION, SHARING, OR SALE.

## MAINTAIN UPDATED POLICIES AND TRAINING

In addition to updating IT policies and processes in regard to responding to consumer requests, your organization should educate employees whose jobs require them to interact with customers. Points of particular emphasis should include the CCPA's definitions of personal information, what constitutes a "California" resident, and how to handle consumer requests. It's also useful to understand that a person may be protected by the CCPA but not be immediately in California. In an increasingly digital work environment, the domiciles of remote personnel can be difficult to determine.

## EXERCISE EFFECTIVE CYBERSECURITY PRINCIPLES

It is advisable to deploy reliable security technologies and methodologies to ensure your organization can technically comply with the CCPA. As more privacy regulations are enacted globally, it's become clear that the future of privacy will be one of strict frameworks and substantial penalties for violations.

Because the CCPA protects the consumer's right to sue for violations, individuals can seek damages in the event that their personal information is breached or otherwise exposed due to inadequate security procedures or practices. This can result in monetary loss for noncompliance and for organizations that suffer a breach.

Fortunately, there are solutions available that can drastically reduce the burden of compliance and the impact of a breach. The CCPA specifically mentions redaction, deidentification, and pseudonymization as methods for protecting the privacy of personal information.

**MONETARY LOSS**

INDIVIDUALS CAN SEEK DAMAGES IN THE EVENT THAT THEIR PERSONAL INFORMATION IS BREACHED. THIS CAN RESULT IN MONETARY LOSS FOR NONCOMPLIANCE.

## PSEUDONYMIZATION

In order to desensitize or de-identify information, companies commonly choose to employ anonymization or pseudonymization. However, fully anonymizing a data set is a difficult task, and once it's done, the anonymized data is useless for almost anything but very high-level data aggregation or analysis.

Because the data's business utility likely was the reason your organization was processing it in the first place, this isn't a terribly attractive solution. Although it is not impossible to deanonymize anonymized data, it does require extensive data-mining efforts in order to return enough information to make cross-referencing feasible—which defeats the purpose of anonymizing data to begin with.

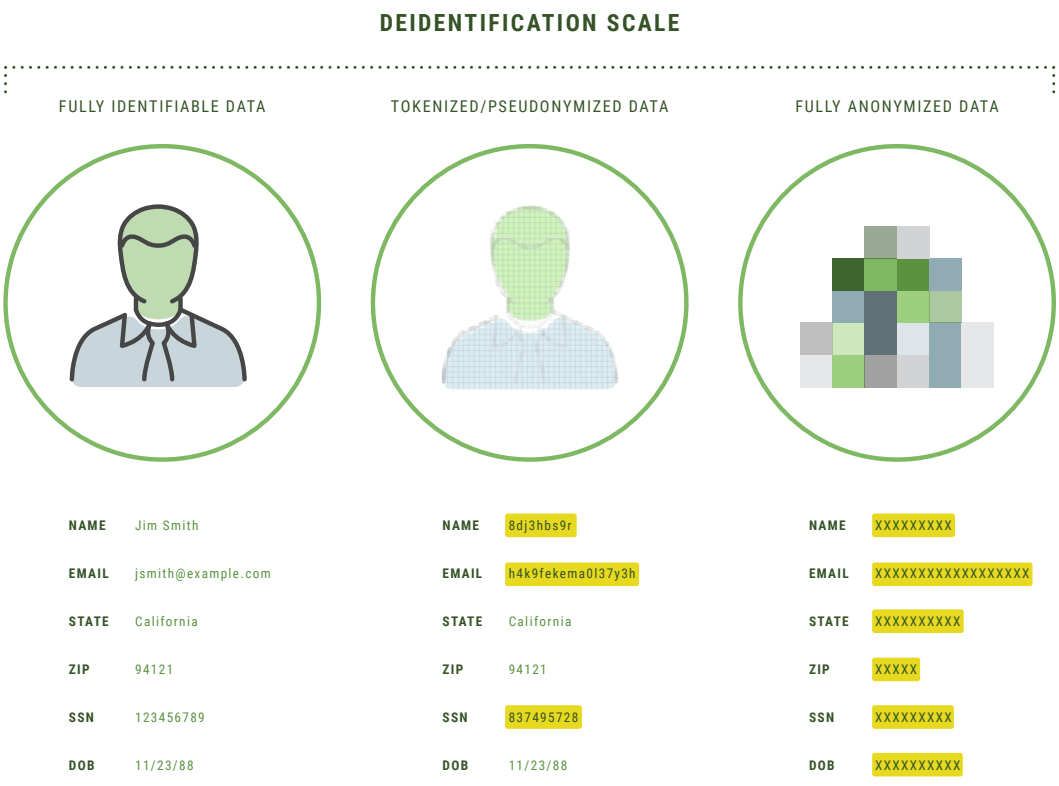
An alternative that "cleanses" sensitive data while still maintaining its valuable business-intelligence purposes is pseudonymization. Pseudonymization is an especially powerful tool for security and compliance. In short, it is the process of deidentifying personal information in a manner that renders it no longer attributable to a specific person (citizen, customer) without the use of additional and separately secured information. This additional information is subject to technical and organizational measures so that the process cannot be reversed to expose the personal data.

Tokenization, a data protection measure TokenEx has been providing for more than a decade to hundreds of organizations across the globe, is an acknowledged and accepted form of pseudonymization.

**PSEUDONYMIZATION**
PROCESSING PERSONAL INFORMATION IN A MANNER THAT RENDERS THE DATA NO LONGER ATTRIBUTABLE TO A SPECIFIC PERSON.

Leveraging TokenEx's industry-leading Cloud Security Platform, TokenEx clients pseudonymize identifying elements of personal information in their internal systems via cloud-based tokenization by replacing it with nonsensitive, randomly generated placeholders. Further, we maintain rigorous internal policies that dictate the appropriate access and handling of tokens to prevent exposure and reidentification by unauthorized parties.

In addition to simplifying compliance, tokenization can reduce the impact of a breach and virtually eliminate the risk of data theft. Because tokenized data cannot be reidentified without additional information and access, a breach of a tokenized environment reveals no sensitive data. Exposed tokens are worthless to cybercriminals and cannot be returned to their original sensitive form, providing protection from theft in the event of a breach. In effect, organizations that use tokenization to deidentify their personal information can help protect themselves against breach notifications, lawsuits, and other CCPA penalties.



## TOKENIZATION VS. ENCRYPTION

Compared to other data protection technologies such as encryption and masking, tokenization is superior due to its ability to retain aspects of the original data, to operate without key management, and to protect your organization in the event of a breach. Whereas tokenization exchanges sensitive data for a randomly generated value, encryption replaces sensitive values with mathematically derived stand-ins.

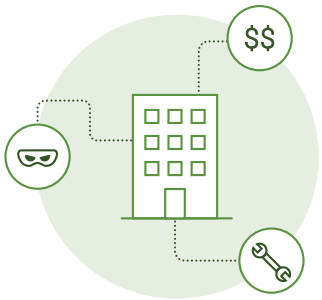
Ideally, encrypted values can only be decrypted and read by an authorized entity which has the same encryption keys that were used to create the value. However, if the keys fall into the wrong hands, an unauthorized party can use those encryption keys to decrypt the encrypted data. The strength of the encryption is based on the algorithm it uses to secure the data—a more complex algorithm will create stronger encryption that is more difficult to crack.

| TOKENIZATION | | ENCRYPTION |
|---|---|---|
| Removes sensitive data entirely, swapping it with a mathematically unrelated "token" | | Uses complex algorithms to obfuscate sensitive data |
| Uses a secure database to vault sensitive data, which can then be retrieved according to the token issued | | Requires a "key" to decrypt cipher text back into its original form |
| Cannot be reversed | | Can be reversed if key is intercepted or discovered |
| Advantage is ease of use | VS | Advantage is securing large or unstructured data sets |
| Reduces PCI DSS, HIPAA, GDPR, GLBA scope | | Does not reduce PCI DSS, HIPAA, GDPR, GLBA scope |
| Secures structured data | | Secures structured or unstructured data |
| Increased business-enablement via analytics | | Presents business-as-usual difficulties |
| No keys required | | Key-management required |

## CLOUD VS. ON-PREM

Cloud-based tokenization platforms offer a cost-effective, scope-reducing alternative to legacy systems. Unlike traditional on-prem security, cloud-based models do not require organizations to incur the ongoing costs and maintenance requirements of on-prem security hardware. This can drive significant savings for development, integration, and infrastructure, while further reducing risk and compliance scope by removing sensitive data from an organization's environment. It also can result in consistent, predictable pricing with the flexibility to scale.

Additionally, entrusting the protection of your sensitive data to security and compliance experts such as TokenEx can improve your security posture and resiliency without inhibiting crucial business processes or other internal operations. That means your organization can benefit from hardened security that enables positive business outcomes.




### ON-PREMISES

**FULL SCOPE**

Stores sensitive data internally
Unpredictable pricing
Internal breach exposes sensitive data
Assumes full liability

### CLOUD-BASED

**MINIMAL SCOPE**

Stores sensitive data externally
Predictable, usage-based pricing
Internal breach reveals no sensitive data
Shifts liability to provider

## WHY TOKENEX?

As the industry leader in tokenization, TokenEx can secure any structured data set—including virtually any type of sensitive data—to effectively achieve full deidentification via pseudonymization. TokenEx can enable organizations around the world to achieve GDPR- and CCPA-compliance by ensuring the security of personal information and data without sacrificing valuable analytics, business intelligence, or the ability to readily delete or retrieve records.

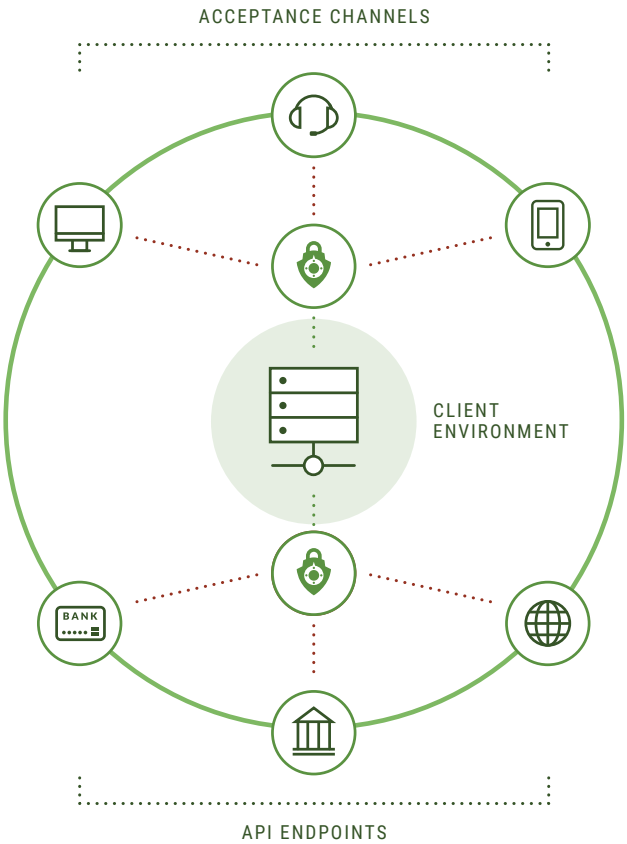
Founded in 2010, our platform was developed by security and compliance experts. We leverage our advanced industry knowledge and technological capabilities to consult with our clients, understand their unique internal systems and processes, and tailor solutions to them.

---

**ACCEPTANCE**
Your customers' sensitive personal and/or payment data is captured at the point of entry.

**TOKENIZATION**
You receive a token for internal use while the original data is safely stored outside of your environment.

**SECURE TRANSMISSION**
You can use our Transparent Gateway to send fully secure and desensitized data to any API endpoint.



When evaluating a tokenization provider, it can be difficult to compare similar technologies and services. Many vendors claim to offer comprehensive solutions, but they often specialize only in certain implementations. Further, not all of them have the necessary experience and expertise to design and deploy tokenization in a manner that meets your specific needs for operational success. TokenEx, however, does possess these crucial qualities for architecting solutions for data protection that enable your desired IT and business functionality.

For more information about our platform or our technology, please reach out to us at **info@tokenex.com**. To learn more about how TokenEx can help your organization comply with CCPA, schedule a call with one of our security and compliance experts today. We'd be happy to help you find a solution that fits your unique needs.



**START YOUR COMPLIANCE JOURNEY TODAY**

Learn how TokenEx can help protect your sensitive data.

REQUEST A FREE DEMO

# KEY TERMS & CONCEPTS

## PERSONAL INFORMATION

Personal information is information that can identify or be reasonably linked with a specific California citizen or household. The term "household" broadens the established interpretation of what constitutes personal data, but much like the GDPR, the CCPA's definition of personal information includes:

- Identifiers such as name, alias, address, IP address, email, account name, Social Security number, driver's license number, passport number, or other similar identifiers.
- Any categories of personal information described in subdivision (e) of Section 1798.80 of the California Civil Code. Many of these categories are covered in the previously listed data set, with the inclusion of payment card information (PCI), protected health information (PHI), employment and education information, and other private personal information from government records.
- Commercial information such as property records, products or services purchased, or other purchasing or consuming histories or tendencies.
- Biometric information such as fingerprints, facial features, DNA, or retina scans.
- Internet or other electronic network activity information such as browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement.
- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.

- Inferences drawn from any of the information identified above. This can be summarized as the creation of consumer profiles reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

## BUSINESS PURPOSES

Under the CCPA, organizations will have to demonstrate that their need for personal information is reasonable and/or necessary to perform the operations for which the information was collected and processed. An example would be an organization that needs to collect personal information to authenticate a customer so that a fraud prevention platform could qualify legitimate transactions and flag or deny nefarious transactions.

1. Auditing or verification for transaction purposes
2. Detecting security incidents, illegal activity, or fraud prevention
3. Debugging to identify and repair errors
4. Short-term transient use
5. Performing services on behalf of the business or service provider, for example:
    a. Maintaining or servicing accounts; providing customer service, order fulfillment, customer verification, payment processing; providing financial analytics, marketing, etc.
    b. Internal research for technological development
    c. Quality and safety assurance of services or a device

## CONSUMER RIGHTS

Under CCPA, every California resident (consumer) has the right to understand and control how its own private information is obtained and stored by any organization, regardless of state or country of operation. It is the burden of the business to be able to provide or delete personal records, or explain how, why, when, and for what purpose they were obtained. Additionally, if a business intends to give or sell California residents' private information to a third party, individuals have the right to opt out.

Under the CCPA, all California residents will have the following rights, enforced by the Attorney General of the State of California:

- Right to know all data about you collected by a business.
- Right to opt out of the sale of your information.
- Right to delete your data.
- Right to be informed of what categories of data will be collected about you prior to its collection and to be informed of any changes to this collection.
- Mandated opt-in before sale of children's (under the age of 16) information.
- Right to know the categories of third parties with whom your data is shared.
- Right to know the categories of sources of information from which your data was acquired.
- Right to know the business or commercial purpose of collecting your information.
- Private right of action when companies breach your data, to ensure these companies keep your information safe.

### PENALTIES

In the event that a business fails to remedy a violation within 45 days of notification, the California Attorney General may impose a maximum of $7,500 per violation for intentional violations. In the event of a breach, any consumer may pursue action to recover damages of up to $100-750 per incident or actual damage, whichever is greater.

## CCPA VS. GDPR

We've talked broadly about the similarities shared between CCPA and its European counterpart, the GDPR, but despite these commonalities, the two regulations differ in several key areas. We'll cover these distinctions below.

### OPT-OUT VS. OPT-IN

Perhaps the most prominent difference between the regulations are their requirements for individual consent. The GDPR requires organizations to obtain consent from EU residents before collecting their personal information for business purposes. In contrast, CCPA requires businesses to provide California residents with the ability to quickly and easily opt out. This effectively places the onus on each individual to revoke permission rather than requiring the organization to obtain consent.

## ORGANIZATIONAL COMPLIANCE QUALIFICATIONS

Although both GDPR and CCPA are extraterritorial in scope and application, there are different requirements for organizations that are subject to the two privacy regulations. GDPR applies to any organization that obtains personal information pertaining to EU citizens. Under the CCPA, only organizations that collect the data of Californians and meet the following conditions must comply:

- Annual gross revenue in excess of $25 million
- Annually buys, receives, sells, or shares 50,000 or more sets of personal information
- Sales of personal information account for 50 percent of annual revenue

## DATA SUBJECT ACCESS

The CCPA and GDPR both require organizations to provide data subjects with access to the categories, sources, purpose, and types of data stored. However, CCPA gives covered entities 45 days to comply with these requests after they have been verified, whereas the GDPR allows for a response time of only 30 days.