KuppingerCole Report

WHITEPAPER

by Martin Kuppinger | November 2019

California Consumer Privacy Act: The Need for Data-Centric Security

CCPA is the latest in a series of global privacy regulations. It comes with new requirements for dealing with personal data and is accompanied by severe penalties. Thus, businesses must take appropriate action to comply with CCPA. While handling consent and opt-outs are at the forefront, successful mitigation of risks starts with data-centric security – it is about understanding where personal data resides and encrypting or anonymizing that data whenever possible. This is where technology, such as data tokenization becomes an essential element for every business.

by **Martin Kuppinger**
mk@kuppingercole.com
November 2019

Commissioned by comforte AG

Content

Related Research

Leadership Compass: Database and Big Data Security – 79015

Executive View: Comforte AG SecurDPS Enterprise – 80007

Whitepaper: Big Data Analytics – Security and Compliance Challenges in 2019 - 80072

1 Introduction

Regulations impact the way businesses operate, but also how technologies evolve. Over the past few years, a series of new data privacy regulations have started impacting businesses around the globe more than ever before, while also leading to technological advancements. One of the latest regulations in that series is the California Consumer Privacy Act (CCPA). Coming into effect on January 1st, 2020, CCPA raises the bar on processing and selling personal data for businesses in California, but is expected to have a broader impact beyond the state of California. Businesses must take appropriate organizational and technical actions to comply with CCPA and to limit the consequences in case of data breaches and fraudulent use of data.

With potentially very severe fines, it is essential to mitigate these consequences. This will require, beyond an adequate organization with defined accountabilities and responsibilities and good processes, policies, guidelines, and controls in place, a well-thought-out set of technologies that help in both complying with CCPA and mitigating the scope and consequences of potential incidents.

Such technologies include tools to manage consent and opt-in/opt-out. They include data discovery for both structured and unstructured data. They include IAM (Identity and Access Management) for limiting access to systems holding personal data.

And they also include technologies for de-identification of personal data: Tokenization, format-preserving encryption, or data masking.

This enables adequate data protection and it helps to anonymize such data. It is important to note that anonymized data is not considered personal data anymore.

Businesses should take CCPA very seriously. The penalties are severe, involving class action lawsuits for damages. The less data that can leak, the lesser the potential damage. Thus, a little bit of consent and opt-out handling is far from sufficient for effective mitigation of CCPA related risks, just as that wouldn't be sufficient for GDPR and other global privacy regulations. It requires a broader perspective, starting by protecting data itself.

Data tokenization is of specific interest because it helps businesses in balancing their need for processing personal data with the requirements of adequate data protection. In many use cases, anonymized data is sufficient to fulfill the business demand, including most scenarios around patient data in clinical trials. Tokenization allows the applications to continue working in the same manner as before, without exposing personal data.

Furthermore, tokenization, data masking, and format-preserving encryption help mitigate the risk of unprotected personal data spreading uncontrollably in an organization. Whoever needs access to personal data in the clear must request it first, which extends security controls to these use cases. This is in contrast to the common scenario of today for many businesses and use cases where personal data is processed and exported to other applications and files and quickly spins out of control. If data is either anonymized or if users must specifically ask for re-identification, it will lead to far greater control of personal data.

We strongly recommend businesses take adequate action for CCPA and related privacy regulations today and think beyond the obvious solutions such as consent management. Without control and knowledge of where personal data resides and how it flows within and beyond the organization, most of the risks of not complying with CCPA will increase. Data-centric security is essential for a successful CCPA strategy.

2 Highlights

- Understanding the impact of CCPA and related privacy regulations and the potential consequences for businesses.
- Six key actions to achieve compliance with CCPA.
- The role of data-centric security for CCPA compliance: discovery and anonymization of data are key to success.
- How tokenization, format-preserving encryption, and data masking help in meeting regulatory requirements of CCPA and mitigating risks of data breaches and fraudulent use of personal data.
- Recommendations for businesses on how to prioritize their actions for becoming CCPA ready.

3 CCPA & more: What regulations require today

CCPA is one of the latest in a series of new privacy regulations across the globe that affects businesses and comes with potentially very severe penalties. It is essential to understand the impact and requirements of CCPA. Specifically, with the potential for class action lawsuits for non-compliance, implementing well-thought-out data-centric security to limit the impact of incidents is crucial.

Regulations have always been influencing businesses and regulations have always been influencing technical evolution. This holds true again these days for the way businesses deal with the privacy of personal data and for the technologies that are and become available in supporting businesses complying with the privacy regulations.

With CCPA becoming effective on January 1st, 2020, businesses must act now

Over the past few years, there have been three major regulations in this area across various global regions. There is the already well-known EU GDPR (General Data Protection Regulation), concerning all business that is done within the EU or affecting EU residents. There is the Singapore PDPA (Personal Data Protection Act), which is relevant to businesses operating in Singapore and appears to be the strictest privacy regulation in APAC. And, finally, there is CCPA (California Consumer Privacy Act), which is part of the California Civil Code and was signed into law in June 2018. CCPA becomes effective on January 1st, 2020.

Thus, businesses need to act now, regardless of which of these regulations may apply to them. For global companies, there is a good chance that all three regulations apply. But even if only one of these applies, the actions to take are fairly similar given that these regulations, while not the same, overlap in major areas. Furthermore, all three come with significant fines for non-compliance and, at least with GDPR and CCPA, a significant risk of being ordered to pay statutory damages.

Without going into the detail of similarities and differences between these regulations: There is a significant overlap, and while GDPR overall is the strictest of these regulations, CCPA also comes with fundamental changes to the way many businesses treat personal data (also sometimes referred to as PII, personally identifiable data) today. Sanctions and remedies are substantial, so businesses should take action to comply with CCPA, but also to adequately protect personal data and to avoid becoming a victim of a data breach.

CCPA, like GDPR, has an extra-territorial scope and is relevant not only to businesses that are resident in California but also to those doing business within California and with California residents.

Like GDPR, CCPA has some extra-territorial scope. GDPR impacts all organizations doing business within EU member states or – and this is where the extra-territorial aspects come in – with EU residents. In consequence, this also affects businesses outside of the EU. CCPA has, in a similar way, a scope on all California residents and businesses acting in California. Again, it doesn't matter where the business resides, but where the individual resides, and the business happens. CCPA is more than a local regulation.

CCPA, like GDPR, comes with a list of key principles and intentions:

- Individuals must be able to gain knowledge about the collection of their personal data.
- They have the right to know whether their personal data is sold or disclosed and to whom. Specifically, the "to whom" part is a key element in CCPA.
- They have the right to block sales of their personal data.
- They have the right to access their personal data.
- They have the right to be forgotten, i.e., requesting the deletion of their personal data if that data is collected directly from the consumer.
- They must not be discriminated against for exercising their privacy rights.

There are several other relevant requirements, such as the need for businesses to implement parental or guardian consent for minors (which technically might become quite complex in implementation), provide links to facilitate the exercise of privacy rights such as "Do not sell my personal information" and to have updated privacy policies. In contrast to GDPR, CCPA works with an opt-out approach for the use of personal data, not an opt-in as GDPR does. However, businesses must avoid requesting opt-in consent for 12 months after an opt-out – which is another requirement that is challenging from a technical implementation perspective.

In contrast to GDPR, there are some more limitations regarding the businesses in scope. The annual gross revenues either must be above US$ 25 million, or the business possesses more than 50,000 records of consumers, households, or devices, or the business earns more than half of its annual revenue from selling consumer's personal data. Factually, the second threshold is the one that will make CCPA applicable to many businesses – for example, 50,000 records of consumer IoT devices is a fairly small number to reach.

CCPA, like GDPR, comes with considerable fines for intentional and unintentional violations, which are up to US$ 7,500 for intentional and US$ 2,500 for unintentional – but per record. Thus, this can add up to very substantial overall fines. For GDPR, the maximum fine is up to 20 million € or 4% of the annual gross revenue of the group, whichever is higher. While there is a cap for GDPR, there is none for CCPA.

Furthermore, there is the right for victims to file class action lawsuits, resulting in statutory damages between US$100 and US$750 per individual, or even greater actual damages. Notably, there is a similar clause in GDPR, which allows for civil lawsuits in addition to the penalties.

When taking all these requirements and potential penalties into account, there is no way to ignore the CCPA requirements. Businesses must act now.

4 Six key actions to take for compliance and protection of personal data

There are many things businesses must do to comply with CCPA. Some are clearly defined, such as links for opting out. Others happen in the background, such as implementing adequate data discovery and a toolset for protecting personal data, from Identity and Access Management (IAM) to data-centric security.

Protecting personal data always starts with the same task: determining where that data resides. Without knowing where personal data resides, there is no way of protecting that data successfully. However, this is only one of six key actions to take for the protection of personal data in the context of CCPA, which are:

1. Discover the PII data you hold
2. Gain control over how PII is accessed and processed
3. Respect opt-outs and gain consent wherever required
4. Ensure that data transfer and cloud storage and processing of personal data comply with the law
5. Detect and notify about data breaches
6. Have adequate organizational and technical actions in place for efficient data protection

Discovery is where everything starts. This is a bigger challenge in today's IT environments than most might think. With Big Data and Analytics, data flows from data sources such as business systems and databases into data lakes, is processed by analytics solutions, and ends up in a variety of formats, from other data lakes to business systems and databases, and various types of files such as Microsoft Excel or PDF reports. Unfortunately, the scope of CCPA is not limited to a certain type of data but affects all. Discovery thus must cover both structured and unstructured data. However, the better you are in the core and source systems, e.g., by masking or tokenization of data, the lower the risks are for the data used in processing.

Discovery is where everything starts. If you don't know where personal data resides, you can't protect if efficiently.

The second point is closely related to IAM, but also to the way Big Data and Analytics environments are managed. It is essential to have adequate access controls and rules of processing in place for personal data, also reflecting and respecting aspects such as consent and opt-outs. In essence, restricting the sprawl of personal data is essential to comply with requirements such as the right for the deletion of data. When unprotected, personal data starts spreading, it is hard, sometimes even impossible, to comply.

Implementing the measures for customers to opt-out and for gathering and managing consent is another important step. This affects customer communication. Businesses are well-advised to demonstrate the benefit of consent and opt-in to their customers. If customers understand the value and that there is a fair balance between why the business wants to use the customer's personal data and why this results in a better service for the individual, the likeliness of consent and opt-in increases.

Another essential action involves the storage and processing of personal data outside the premises of the organization. Accountability and responsibility do not transfer but duplicate when the data leaves the organization. Both the business and the external data processors are affected, with all the accountabilities and responsibility for the customer-facing business remaining in place. Actions here involve contractual and technical measures. Amongst the latter, an important task is restricting and protecting the data that is transferred, e.g., with format-preserving encryption, tokenization, or data masking.

Regulatory compliance with data protection regulations such as CCPA will not be achieved by deploying a single technology, but by having a well-thought-out portfolio of technologies in place, covering all types of data and requirements.

Again being both an organizational and technical action, there is the need to be prepared for data breaches. No matter what actions are taken for prevention, there will always remain a risk of a breach. If a breach happens, the faster a business reacts, the better. Technical measures for minimizing the impact of the breach can be taken faster and more efficiently, and crisis communications, including formal notifications of the data protection authorities and, if required, the affected customers, can happen earlier.

Finally, it is about having an adequate organization and a set of technologies in place for protecting data. The organizational aspects involve, e.g., the DPO (Data Protection Officer) that defines and monitors data protection-related policies and controls, but also the CISO (Chief Information Security Officer), who is in charge of implementing adequate technical measures.

With the wide variety of challenges CCPA and other regulations impose, there is not a single solution that covers all. It is about managing consent and opt-out/opt-in, it is about discovering personal data in both structured and unstructured data, it is about access controls and their governance, and it is about hiding sensitive data, to name just a few major areas. Thus, revisiting the portfolio of technologies and places and filling gaps is essential. Amongst these technologies, approaches that protect PII from being accessible in an unauthorized manner play a central role.

5 Protecting data: Encrypt, tokenize, and continue operating

Data-centric security helps to limit the potential impact of data breaches and fraudulent use of personal data. Anonymization of records by tokenization and masking play a central role therein. It is highly recommended to implement such technologies in the scope of CCPA.

In the list of technologies that are relevant for protecting personal data from leaking and from fraudulent use, one technology plays a major role: Protection of structured data through tokenization, format-preserving encryption, or data masking.

Such protection is essential not only to comply with regulations but for mitigating the negative consequences of non-compliance. If credit card data, health records, and other information that is perceived as being highly sensitive, are affected by violations of data protection regulations and by data breaches, the likeliness of severe fines increases. Furthermore, the more critical data is (or is perceived as being critical), the higher the likeliness of class action lawsuits and the associated damages. Data masking, tokenization, and format-preserving encryption limit the scope of attacks and abuse because the sensitive data is not visible to the attackers and fraudulent users.

Thus, for mitigating the consequences of CCPA, but also for complying with CCPA, it is important to have a closer look at the positive impact of this set of technologies. That specifically holds true for getting a grip on the risk that arises from the sprawl of personal data. If data is encrypted, tokenized, or masked the right way, it anonymizes the data. It is not personal data anymore, and the risk of such data being out of control or leaking is mitigated to a certain extent. If data is anonymized, there is no need to delete it on request. If data is anonymized, a data breach does not affect personal data, but just some of the data.

Obviously, not all data can be anonymized. This depends on the processing requirements for the data. However, a lot of data can be anonymized, masked, tokenized, or encrypted. Anonymization in that context is a result of applying technologies such as masking or tokenization. A common use case is for patient data used in clinical trials, where the researchers might need access to a huge amount of clinical records, but all the relationships to the individuals might be removed in a way that the records are anonymized. They might indicate age and sex, but no names, birth dates, addresses, or other elements that allow an individual to be recognized.

Technologies for data encryption, data tokenization, and data masking are essential elements of every well thought-out approach to cybersecurity and regulatory compliance.

Masking in that context is a fairly simple approach. It just replaces parts of the data by other data, e.g., random data, simple characters as “x”, or others. The challenge with data masking is that, while it requires little processing power, it might affect processing. This starts with check digits, e.g., in credit card numbers – just replacing it with a random number of characters will affect applications that check for the (theoretical) validity of such credit card numbers. That is where tokenization comes into play.

Tokenization replaces the original data in a format-preserving manner. It still requires fairly low computational power when compared with encryption.

Encryption, on the other hand, leaves data as is but encrypts it. This requires significant computational power and commonly limits further processing of data by applications because it changes the format of the data.

There are some emerging approaches around homomorphic encryption that allow for computing operations on encrypted data, but these are still fairly limited in their applicability.

The practical impact of data tokenization and masking is that uncontrolled data sprawl will be limited, because users must request data access and de-tokenization, thus becoming subject to solid security controls.

When looking at the definition, scope, and the potential consequences of CCPA and other privacy regulations, tokenization and related technologies are an essential element in protecting personal data. They limit the potential impact of data breaches and help to mitigate the consequences of uncontrolled sprawl of such data, be it by data ending up in unstructured documents such as Microsoft Excel files or uncontrolled processing of data in Big Data and Analytics applications. The practical impact will be that sprawl is limited by forcing users to request access to the "real", non-tokenized data when they need it. This allows for implementing controls on the further use of such data, mitigating unwanted and uncontrolled sprawl.

We thus strongly recommend adding data encryption, data tokenization, and data masking technologies to the essential set of tools in use for cybersecurity and regulatory compliance. Notably, the impact of these technologies is way beyond regulations, such as CCPA.

6 Action Plan for meeting the requirements of CCPA

There are several actions businesses must take. It is essential to not only cover the high-level requirements but to use CCPA as a starting point for improving the level of data-centric security across the business, serving more than just regulatory compliance with CCPA itself.

With CCPA becoming effective on January 1st, 2020, there is not much time left to prepare for CCPA. Many businesses are not where they should be and they will not be there on time. This is not a surprise, but a common scenario for new regulations. It happened the same way with GDPR.

Complying with CCPA requires technology, but it is not a technology-first topic. Technology helps, but it requires an adequate organization with clearly defined accountabilities and responsibilities and it requires well-defined policies, guidelines, and controls. DPOs and CISOs must work hand in hand to implement these controls.

As discussed earlier in this paper, we recommend businesses take six key actions to comply with CCPA, beyond the organizational actions to take:

1. Discover the PII data you hold
2. Gain control over how PII is accessed and processed
3. Respect opt-outs and gain consent wherever required
4. Ensure that data transfer and cloud storage and processing of personal data comply with the law
5. Detect and notify about data breaches
6. Have adequate organizational and technical actions in place for efficient data protection

Defining a well thought-out portfolio of technologies that help in these key actions is essential. Technologies for data discovery are part of that, but also technologies that help in encryption, tokenization, and masking of data. The less access someone can gain to personal data, the lower the risk involved in data breaches and fraudulent use, and the lower the potential consequences of such incidents.

There is a good reason for technologies, specifically data tokenization, being widely used in the Financial Services industries, for protecting financial transaction data, credit card data, and other sensitive information. With the business risk associated with breaches of personal data increasing due to new regulations, it is time to extend the scope of these technologies.

7 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstrasse 20 - 22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com