PREPARING FOR THE

with

Appsflyer

Introduction

The world is becoming increasingly more private. In the last several years, laws and regulations have tightened on what organizations may and may not do with personal user data.

The GDPR was not the first law to regulate organizations use of users' personal data, but it was one of the most significant; spanning multiple regions and applying to virtually every global organization on the planet, the GDPR forced many companies to rethink how they collect and process user data.

The California Consumer Privacy Act (CCPA) will take effect in 2020, aiming to provide the residents of California with similar rights as the GDPR provided citizens of the EU. The CCPA will require some preparation for organizations that manage personal data, especially those in the mobile industry.

As the industry's leading mobile attribution and analytics platform, AppsFlyer is committed to providing its customers full transparency and control over their users' personal data, empowering them in their pathway to regulatory compliance. As such, we have composed a mini-guide to help organizations prepare for the upcoming CCPA and understand how AppsFlyer's services fit into their compliance efforts.

CCPA, the basics

What?

The California Consumer Privacy Act (CCPA) is a new law, designed to protect the consumer privacy rights for residents of the state of California in the United States.
Similar to the GDPR and other privacy laws, the CCPA is intended to provide individuals (in this case, California residents) with increased control over their data and privacy while imposing increased obligations on businesses.

When?

The CCPA will come into effect on January 1, 2020 and organizations must start preparing to ensure they are able to meet the compliance challenges that the CCPA presents.
The CCPA is a state law that was adopted by the California legislature on June 28, 2018. While the bill was signed on June 28, 2018, the law itself becomes operational January 1, 2020, with enforcement by the California Attorney General beginning July 1, 2020. What this means is that residents may already start making requests under the CCPA starting January 1, 2020, however the Attorney General Office of California who is responsible for enforcing the law will not begin to do so until July 1, 2020.

Who?

While the CCPA is a California state law, it can apply to any organization around the world that meets the criteria. The CCPA applies to any organization ***that does business in California**** and meets the following conditions:

(1) is for-profit
(2) collects personal information of California residents
(3) **determines the purposes and means of the processing** of consumers' personal information; and
(4) satisfies one or more of the following thresholds:

- Has annual gross revenues in excess $25,000,000.
- buys, receives, sells, or shares for commercial purposes, the personal information of 50,000 or more consumers, households, or devices.
- Derives 50 percent or more of its annual revenues from selling consumers' personal information

*"Doing business in California" should be interpreted broadly to include anyone who collects or sells personal information of California residents.

CCPA, the basics

Why?

The international focus on consumer privacy and personal data collection by organizations has garnered a lot of publicity in recent years. It continues to gain traction as the global discussion on data management grows and continues to uncover the extent of use by certain organizations. The GDPR was one of the most significant laws to be passed, shifting entire industries to rethink how they manage user data. More laws of this sort are expected to follow in coming years.

Details, implications and penalties

- Wide territorial scope such that even companies outside of CA will be subject to the law
- Broad definition for “personal information”
- Strict obligations regarding transparency
- Increased data subject rights including access, deletion and opt out rights
- Penalties for breaches and private action rights

What rights do consumers have under the CCPA?

(a) **Transparency Rights:** Consumers have a right to receive certain information about how a business collects and uses their information. Such information must be provided within a privacy policy and upon request.

(b) **Right of Access:** Consumers have a right to request access to certain information which includes categories of personal information collected or sold, specific personal information, sources, purpose of collection and use and categories of third parties that the Business sold personal information to.

(c) **Portability Rights:** Consumers have the right to receive the information in a readily useable format that allows consumers to easily transmit the information to another entity.

(d) **Right of Deletion.** Consumers have a right to request deletion of data collected from them. Upon such request, a business must delete such data (subject to certain exceptions) and flow down the request to its service providers who must comply.

(e) **Right to Opt Out.** Consumers have the right to require any business that sells information to third parties to opt out from selling their information. In the case of personal information of children between 13-16, a the child must opt in to permit such sale and under 13 must obtain parental consent.

(f) **Non-Discrimination Rights.** Subject to certain exceptions businesses are prohibited from discriminating against any Consumer who exercises a right granted under the CCPA and must continue to provide equal service or goods and price even if one exercises his rights.

Details, implications and penalties

What personal information does the CCPA apply to?

The CCPA applies to personal information of Consumers (i.e. California residents) where the term, "personal information" is defined broadly as follows:

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

Some examples specifically mentioned in the CCPA include:

- name, alias, address, email address
- unique and online identifiers, IP address
- government ID's
- records of personal property, products or services purchased or considered
- consumer purchasing or consuming histories or tendencies
- biometric information
- browsing and search history
- interactions with an Internet Web site, application, or advertisement
- geolocation data
- professional or employment-related information

Penalties for non-compliance

Organizations found in violation of the CCPA will be charged a penalty. Penalties are:

- $2,500 for each violation
- $7,500 for each intentional violation

Don't be fooled by these seemingly low numbers; a violation will likely occur per consumer and these fines may easily reach millions. However, businesses will have a 30-day cure period to correct the violation prior to the action commencing.

In addition, individuals have a private right to action in certain cases where their unencrypted or unredacted personal information has been exposed **due to a business's failure to maintain reasonable security safeguards**. While the scope is more limited, individuals may seek statutory damages between US$100 to US$750 dollars per violation which may be brought in class actions.

As a business subject to the CCPA, what should we do?

Given the wide scope of the CCPA it is likely to affect many businesses. Therefore, businesses must take some basic steps to ensure they are compliant.

Getting started - important steps

1. Determine what personal information the business processes.
2. Determine the purposes for which such personal information was collected or received
3. Determine how that information is actually being used
4. Determine if the information is being shared with anyone and if so with who and for what purpose
5. Determine whether you use any service providers and whether you have appropriate agreements in place with such service providers that meet the requirements under the CCPA
6. Determine whether you are selling (as such term is broadly defined in the CCPA) any personal information and if so whether any such information is from children
7. Determine all the storage points of such information and whether accessible for the purpose of access requests and deletion requests.
8. Determine whether you have a process to accept requests from consumers and to act on such requests
9. Determine whether your privacy policy is up to date containing all disclosures required under the CCPA

As a business subject to the CCPA, what should we do?

Once your business has taken the steps above, it will be better prepared to fill the gaps to ensure compliance. Some important operational requirements under the CCPA include:

Important steps to take toward CCPA

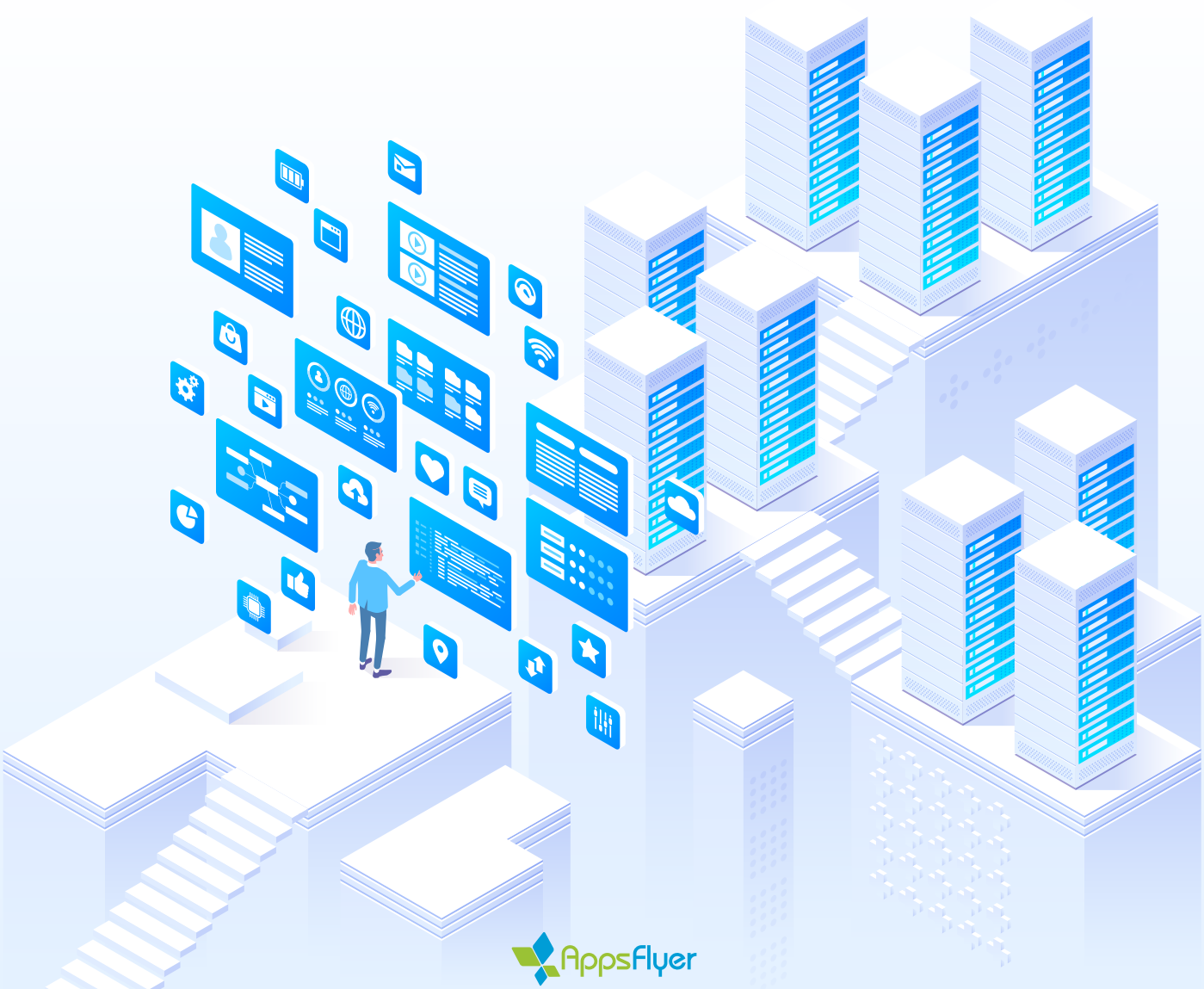
- Providing at least 2 methods for consumers to make requests, one of which must be a toll-free phone number. The other must be made available through a website when one exists.
- Providing a conspicuous link on the bottom of your homepage and within privacy policies titled “Do Not Sell My Information” which leads to an opt-out for selling personal information
- Providing an updated privacy notice that includes:
    - a description of a consumer’s right to request information regarding the collection and sale of his personal information as well as his deletion and opt out rights;
    - the categories of personal information collected and if sold or disclosed then such categories sold, or disclosed for a business purpose, in the preceding 12 month period;
    - sources;
    - purposes of collection or sale;
    - categories of third parties data shared with;
    - specific pieces of personal information it has collected about that consumer;
    - methods to make disclosure requests; and
    - any financial incentive program
- Provide training to employees on how to ensure compliance with the CCPA including the handling of consumer requests

If we comply with the GDPR, are we ready for the CCPA?

The GDPR, which came into effect in May 2018, forced many organizations worldwide to make actionable changes in the way they handle user data.

Any business that prepared itself for the GDPR may have a head start for CCPA compliance but will not be fully compliant under the CCPA. While there are some similarities and overlaps between the two laws, they are still very different and thus require different operational implementations. Areas where you may leverage your GDPR readiness include:

1. Data mapping
2. Processes to receive and handle data subject requests
3. Methods to delete personal information
4. Methods to provide access to personal information in readily useable formats
5. Technical and organizational measures used to protect personal information
6. Privacy notices



Helping our customers prepare for the CCPA

AppsFlyer as a service provider

Many organizations that will need to meet CCPA regulation requirements are using AppsFlyer's attribution and marketing analytics services.

> **Under the CCPA, the act of disclosing information to an entity that processes personal information on behalf of the business for a business purpose (as defined under the CCPA) is permitted and will not be deemed as "selling" under the CCPA.**

The entity receiving personal information for such purpose is called a "service provider".

AppsFlyer's compliance program

AppsFlyer has offered (and continues to expand) an unparalleled global compliance and certification program, meeting the strictest industry standards when it comes to security and privacy. This compliance program is part of the greater privacy initiative lead by AppsFlyer, ensuring to our customers that AppsFlyer is a compliant service provider they can rely on and trust.

AppsFlyer's commitment

AppsFlyer designs products with privacy and security at their core. We are committed through-and-through to the principles of privacy: transparency, accuracy, data minimization and accountability.

As data processors, we continuously provide our customers with the infrastructure as well as education on best practices, compliance, policies and industry trends in order for them to provide the optimal experience for users — which includes protecting against data breaches, infringement on privacy and other concerns.

Helping our customers prepare for the CCPA

AppsFlyer welcomes the movement towards more stricter regulation on data privacy, and proudly aligns with global regulations. We work to help our customers be compliant as well, providing them with what they need from a privacy perspective to be compliant.

To help our customers ensure compliance with the CCPA AppsFlyer is committed to:

1. Acting only as a service provider for our customers and processing the data only for the stated business purposes
2. Never selling or disclosing any personal information received from our customers
3. Being fully transparent with our customers
4. Supporting customer opt-in and opt-out requirements
5. Supporting all data deletion and access requests
6. Ensuring appropriate agreements are in place with our customers
7. Having appropriate technical and organizational measures in place to protect our customer data

OpenGDPR

OpenGDPR is a universal, secure, and common framework for compliance with GDPR mandated data subject rights. Developed in partnership with MarTech leaders, The OpenGDPR framework presents a public API specification along with a recommended set of best practices for implementing and maintaining a connected and compliant stack. By adopting OpenGDPR, brands can reliably address data deletion and access requests across their partner ecosystems, in near real-time.

Data access and deletion are fundamental aspects in both the GDPR and the CCPA. OpenGDPR makes this aspect of compliance easy and accessible to all.

For more information on AppsFlyer readiness and preparation for the GDPR and CCPA, visit our website.

AppsFlyer