China’s Personal Information Protection Law
A word from our lawyers: Nothing stated here is legal advice. It is provided for your information and convenience. We strongly encourage that you work closely with legal and other professional advisors to determine exactly how the China Personal Information Protection Law applies to you.
Background of the PIPL:
On November 1, 2021 a new data protection law came into effect in China - the Personal Information Protection Law (“PIPL”). Together with the already existing China Cybersecurity Law and the recent China Data Security law, the PIPL is part of the comprehensive framework for data protection being established in China.

The PIPL bears many similarities to the EU’s GDPR. It applies to the processing of personal information of natural persons within China (not just Chinese nationals); however, similar to the GDPR it also has an extraterritorial scope (for example where the the activities conducted outside of China are intended to provide domestic individuals with products/services; or where their activities are analyzed). Therefore, even companies outside of China doing business in China will need to be aware of and comply with the law.

Scope of Application:
The definition of Personal Information under the PIPL is broad and includes all kinds of information related to identified or identifiable natural persons recorded by electronic or other means. Anonymized data has been specifically excluded.

The primary obligations under the PIPL are on the “personal information handlers” which is akin to the GDPR’s data controller. Data processors under the GDPR are called “entrusted parties” under the PIPL. Under the PIPL, AppsFlyer would be considered an entrusted party.
Guide to compliance in respect of using AppsFlyer:

Customers of AppsFlyer are deemed the personal information handlers under the PIPL and will have the primary responsibility for ensuring their compliance with the PIPL.

Customers will first need to establish a lawful basis to collect personal information from their end users. Some of the lawful bases covered under the PIPL are similar to those under the GDPR – for example, to conclude or perform a contract to which the individual is a party; to perform legal duties; health emergencies; and public interest.

However, the most appropriate lawful basis to cover a customer’s use of AppsFlyer will likely be consent. This is due to the fact that the PIPL does not have a GDPR like “legitimate interest” lawful basis. As a result customers will need to make sure to obtain appropriate consent from their users in respect of their collection of personal information.

In order to obtain appropriate consent, customers will also need to provide their end users with proper notice of their data collection and use practices. Customers may view AppsFlyer’s Service Privacy Policy to gain a broader understanding of the categories of data processed by AppsFlyer on behalf of customers.
**Cross border transfer:**

One of the more spoken about issues covered under the PIPL relates to cross border transfers of personal data. Since AppsFlyer operates its servers in the EU where its processing complies with the most stringent data protection laws including the GDPR, customers of AppsFlyer will need to take the necessary steps to ensure they are able to transmit data to AppsFlyer.

Fortunately, under the PIPL, several frameworks and conditions have been provided to allow personal information to be sent and processed outside of China. This is a big development which will enable companies operating outside of China to continue to provide services in China. The core condition for cross border processing is the need for the personal information handler to provide specific notice and obtain specific consent from its end users to transfer data outside of China. Customers of AppsFlyer should be sure to provide such notice and obtain the necessary consent.

In addition, the transmission of personal information outside of China will need to be covered by one of the frameworks provided under the PIPL:

1. Security assessment and approval by the Cyberspace Administration of China (CAC) (this will be required for Critical Information Infrastructure (CII) operators and those handlers processing an amount of data that exceeds a threshold to be set by CAC); or
2. Certification by approved bodies; or
3. Concluding a contract with the body processing the data outside of China on terms set by CAC - Similar to the EU’s Standard Contractual Clauses.

The most likely framework that will be appropriate for most non CII AppsFlyer customers will be concluding a contract with standard clauses set by CAC. While CAC has yet to provide such a standard contract (or a process for certification or security assessments), it is expected that final guidance will be coming soon.
**AppsFlyer's DPA and data processing:**

In the meantime, customers can feel confident that AppsFlyer will continue to process personal data in accordance with the stringent requirements of the PIPL and other global laws. Besides AppsFlyer operating as an entrusted party and not using the personal data for any reason other than to provide the services requested by the customer, AppsFlyer provides a special data protection addendum to cover its processing of the personal data. The DPA covers a range of issues such as AppsFlyer's commitment to implement appropriate technical and organizational measures to protect personal data, to assist customers with their compliance needs including by cooperating in respect of data protection impact assessments, individual rights request (such as the right of deletion), breach notification requirements and more.

We also note that the nature of the data AppsFlyer needs to receive in order to provide the services does not include any sensitive or direct personal information and is limited to personal data that is pseudonymised by nature (e.g. advertising device ID's, IP's. Therefore, we are confident that our existing measures will be sufficient to ensure complete compliance with PIPL requirements. Indeed, customers will need to also assess any additional laws applicable to them given their own products since certain unique industry specific obligations may apply to them in addition to the PIPL.

**Individual Rights**

Once data is transmitted to AppsFlyer, AppsFlyer enables customers to comply with their obligations under the PIPL in respect of individual rights - specifically, AppsFlyer provides the OpenGDPR framework to enable customers to automatically submit individual deletion and data access requests.

AppsFlyer is also committed to maintaining appropriate internal management systems and operating procedures as well as appropriate technical security measures to protect customer data. For more information on such measures please visit our Trust Hub.
**Future Compliance:**

As a final note, the PIPL is a comprehensive law and has a broad set of obligations – for example requirements to appoint special data protection officers, perform data protection assessments (including for profiling related to targeted ads), rules regarding automated decision making and more. Therefore it is important that every customer assess the PIPL with their advisors taking into consideration the nature of their own services and take the necessary steps to ensure compliance. AppsFlyer is here to assist you in ensuring such compliance. Be assured that AppsFlyer is continuously monitoring the developments around the PIPL, its enforcement and the cross border frameworks and is working diligently to ensure that customers will be able to continue to use AppsFlyer in full compliance with the PIPL and other global laws.