Implementing a compliant attribution solution for kids apps with AppsFlyer

Introduction

When collecting data from children, app developers need to consider a wide range of platform policies, regulations, and laws that are in place to protect children. Some of these laws are specific to children (COPPA) while others are broad but provide specific protections for children (GDPR and similar local laws). Additionally, in recent years platforms such as iOS and Android have implemented specific policies and rules to help provide improved safety and privacy for our children.

At AppsFlyer data privacy is at our core. We strive to be at the forefront of the industry's privacy standard and work to pave the way for heightened security and privacy standards most specifically towards apps that have children as all or part of its audience.

Our state-of-the-art and innovative infrastructure along with our core governing data protection, certifications, and regulatory compliance have earned the trust of the world's leading brands.

The following is information and a set of guidelines and options available to you when integrating AppsFlyer's kids directed solution in your app that will help support your compliance with data protection laws such as GDPR and COPPA as well as various platform policies.

Please make sure to implement the appropriate controls for your apps audience to ensure your compliance.

The controls

AppsFlyer provides a wide range of controls and tools to support compliance with the various child data protections laws and platform rules. The controls range from limiting AD ID collection to not collecting any data. You also have the ability to collect and transmit data to AppsFlyer for attribution and analytics purposes while limiting or completely blocking data you share with third parties through AppsFlyer.

AppsFlyer's controls will support any internal implementation for compliance that you have chosen.

To help you please follow these guidelines:

1. **Choosing the SDK and Advertising ID configurations**

iOS - Apps in kids category or primarily directed to kids

For iOS AppsFlyer has developed a dedicated SDK for apps in the kids category or primarily directed to children called the Strict SDK. The Strict SDK for iOS is a version of the SDK that doesn't contain a dependency to Apple's AdSupport Framework and does not collect IDFA from the device under any circumstance. To learn how to download and install the iOS SDK with a detailed step-by-step guidance for developer implementation click here.

Please note the following when using Strict Mode:

a. Strict SDK will prevent IDFA collection but IP addresses may still be received and, therefore; all additional controls set forth in this guide (e.g. Prevent Data Sharing) still need to be considered for COPPA and GDPR compliance.

b. Attribution with SRN's is not possible with Strict SDK

iOS - Apps with children as part of their audience

If your app is not intended primarily for kids but instead targets children as part of your audience, you may utilize the standard iOS AppsFlyer SDK. However, COPPA requires you to obtain parental consent where you have knowledge that you are collecting children's personal data unless one of the COPPA exceptions is met. Therefore, if you are targeting kids as well as adults you should implement a relevant age gate in your app to ensure that the SDK configuration for users identified as children is compliant (see below options for more information). If you choose not to implement an age gate you will need to ensure all other controls are in place to ensure compliance with COPPA and GDPR (e.g. Prevent Data Sharing).

Android - Apps targeting kids only or kids as part of the audience

As part of your app submission, Google requires app developers to identify the audience they target. If the target audience is kids only, then, the AAID should not be collected. Unlike iOS, for Android there is no Strict SDK, and therefore, app developers will be required to set the <setDisableAdvertisingIdentifiers> API prior to calling 'start', at which point the SDK will not be enabled to collect the AAID. For more information on how to implement this control click here.

If the app targets children as part of the audience, then you should implement a relevant age gate in your app to ensure that the SDK configuration for users identified as children is compliant (see below options for more information). If you choose not to implement an age gate you will need to ensure all other controls are in place to ensure compliance with COPPA and GDPR (e.g. Prevent Data Sharing).

SDKless solutions

There is an option for you to utilize SDKless, server to server implementations, which enables you to configure on your own servers what data will be sent to AppsFlyer. If you choose to use this method, you must ensure compliance with COPPA & GDPR regulations.

SKAN only (iOS)

An option available to iOS targeted campaigns is to utilize attribution only through Apples SKADnetwork (SKAN). When utilizing only SKAN (and not implementing Apple's ATT consent framework), then by default the only data shared with third party networks is aggregated data as no Advertising ID is available to any party including you and AppsFlyer. To limit use to SKAN you may utilize the appropriate SDK as identified above and submit a request to your Customer Support Representative. Please note that due to the customizations required this option is only available for accounts with a subscription fee of 100k and above.

2. Age-gate and consent framework support for apps with children as part of the audience

As noted above, when app developers are targeting children as part of its audience, they should implement an age gate within their apps to ensure that any personal data designated as coming from children is treated correctly and in compliance with applicable laws and rules such as COPPA and GDPR.

AppsFlyer supports various capabilities when implementing an age gate. This ranges from blocking the collection of any data when a user does not pass the age gate to allowing the data collection but enabling additional controls to be configured to ensure that you do not share data with third parties through postbacks.

When implementing an age gate or any controls dependent on the age gate results, it is critical that any such controls are called prior to the 'start' of the SDK.

SDKless solutions

While less recommended, there is an option for you to utilize SDK less, server to server implementations, which enables you to configure on your own servers what data will be sent to AppsFlyer.

No data collection - opt-in/out

AppsFlyer enables you to configure the SDK so that it 'starts' only for users who pass the age gate (i.e.users at or above the age of consent). This is done by having the SDK 'start' only after receiving a flag that the age gate was passed with an appropriate age. If the SDK is not started then no data will be sent to AppsFlyer from this user. For more information see here.

Collect data

If you wish to collect data regardless of whether a user passes an age gate or not then you will need to ensure that all other controls are in place to ensure your compliance with COPPA, GDPR or other applicable laws and rules.

For example, one such control for COPPA purposes may be that you have determined that your use of AppsFlyer is covered under the COPPA "support for internal operations" exceptions rule and that the data will only be used for analytics purposes. In such a case you will need to ensure that no data is shared with third parties who can use that data for behavioral targeting, profiling or other purposes beyond the exception and therefore you will need to implement the Prevent Data Sharing controls below.

For GDPR purposes, if no consent is requested then you will need to ensure another lawful basis is appropriate, and that if legitimate interest is relied on that an appropriate assessment has been performed.

For GDPR purposes if legitimate interest is relied upon it would be recommended to implement the same Prevent Data Sharing controls as described for COPPA considering that under the GDPR children merit specific protection with regard to their personal data.

3. Prevent data sharing

AppsFlyer provides a few different options to limit the postbacks you send to the ad networks or your sharing of personal data with the third parties you work with. These should be used in all cases where (i) parental consent has not been received as required under COPPA for, among other things, use of a child's personal data for behavioral targeting or profiling; and/or (ii) the third party you are working with has not committed to treating data shared with it solely as a data processor for the limited purposes allowed under any exceptions for consent contained in COPPA, GDPR or applicable laws and rules; and/or (iii) applicable laws or other platform rules require it.

Complete block

To completely block any data from being sent to any third party network that you have configured the service to work with you may use the <setSharingFilterForPartners>("all") SDK method.

Note that you will need to activate this control in the AppsFlyer SDK BEFORE the first 'start' call.

When performed the following will apply to the whole session?

- Users from SRNs are attributed as Organic, and their data is not shared with integrated partners.
- Users from click ad networks (non-SRNs) are attributed correctly in AppsFlyer, but data will not be transmitted to the ad networks via postbacks, APIs, raw data reports, or any other method.

To block data from being sent only to certain partners and not others you may use the ***<setSharingFilterForPartners> ("MediaSourceName").*** This should be used only if some of the third party's you work with have appropriate commitments in place ensuring the sharing of data with them will not breach COPPA, GDPR or applicable laws and rules (for example when you have appropriate consent and/or by acting solely as a processor and using the data solely for analytics purposes on your behalf in line with the exceptions provided under COPPA).

For more information on the above methods you can learn more here.

Aggregated Advanced Privacy - AAP (iOS)

For iOS campaigns AppsFlyer provides an option that enables you to send only aggregated information to the networks where explicit consent to Apple's ATT consent framework was not received, for example in a child directed app where the child can't consent to the collection of their data. This setting is controlled through the dashboard and is on by default. Despite any controls above, as an additional layer of control we recommend not turning this setting off. You can learn more here about AppsFlyer Aggregated Advanced Privacy framework (AAP).

IP masking and post-install anonymization

AppsFlyer enables app developers to analyze what marketing campaign led to an initial install of an app and to attribute any post install event configured by the app developer to the same campaign. Where customers want to ensure attribution measurement is limited only to the initial install and that any event configured post install is not attributed or linked to any marketing campaign they may do so with the requestListener and anonymizeUser (true) controls as further described here.

This method may also be used to hash IP addresses

For more information click here.

4. Additional controls

Data deletion

Do children (or their parents) wish to delete their personal data within your app?

AppsFlyer has developed an API specifically to address any 'data subject requests' across the globe and is committed to assisting in allowing your app users to exercise these requests in a user-friendly manner.

Addressing and managing requests by Data Subjects submitted in accordance with privacy regulations, AppsFlyer, together with mParticle, Amplitude, and Braze, initiated the OpenDSR protocol.

You can learn more here about how to implement deletion requests into your app and the manner in which compliance takes place. From the moment of receipt of a deletion request, AppsFlyer ensures deletion within 15 days.

5. Conclusion

AppsFlyer is committed to protecting our children and to providing you with all the tools and functions you need in order to ensure they are able to remain compliant with the varying platform policies, regulations and laws. As a data processor AppsFlyer will only process your data on your behalf and in accordance with your configuration of the service.

It's important to note that the above guidelines are provided for your convenience to help you ensure you configure the services in compliance with applicable child data protection laws and platform rules. However, it is your responsibility to ensure you fully understand all laws and rules applicable to you and to perform all actions required by such applicable laws and rules to ensure your compliance, including, without limitation, implementing appropriate controls, providing appropriate notices and policies as well as obtaining consent where required.

6. Quick guide

1. Determine who your target audience is - Is it kids only, adults or are you targeting both kids and adults?

2. Choose the right SDK for you based on your target audience:

- Kids only
  - iOS: use the Strict SDK for iOS;
  - Android: use the standard SDK but ensure you utilize the <***setDisableAdvertisingIdentifiers***> function is set
- Mixed audience you may use the standard SDK's but ensure implementation of additional controls as set below

a. Implement data sharing controls:

- Where you want to treat data usage differently based on age you should implement an age gate and apply the appropriate controls based on whether a user passes the age gate or not;
  - If you do not wish to collect any data from users who do not pass the age gate (under the legal age): set a flag and don't apply **'start'** to the SDK for such users
- To use such data solely for analytics attribution purposes and not share postback data with any third party for campaign optimization etc.: use the ***<setSharingFilterForPartners>***
  - For iOS ensure the AAP setting is on as an additional layer of control - ensures that where consent to Apples ATT framework is not provided, data shared with third party networks in postbacks is aggregated.

3. Delete data:

To delete any user's data implement the OpenDSR API.