Google Play Data Safety Questionnaire

Nothing stated herein is legal advice. We are providing the answers below merely for your convenience to assist you in responding to the Google Play privacy questionnaire as we currently understand the guidelines. These answers are limited to the AppLovin/Max/SafeDK SDK and do not cover other functionalities or SDKs that may be present in your applications. App developers are solely responsible for implementing and configuring the AppLovin SDK and responding to the questionnaire in accordance with their specific configurations and uses.

DATA SAFETY

Data collection and security:

Review the list of required user data types that you need to disclose.

Does your app collect or share any of the required user data types?

✓ Yes
□ No

Is all of the user data collected by your app encrypted in transit?

✓ Yes
□ No

Do you provide a way for users to request that their data is deleted?

✓ Yes
□ No

Data types:

Each positive selection of a data type being collected will generate a follow-up response about how and why the data is collected.

Data Type Category	Sub Data Type	Note	Data Required?	Collected	Shared
Location	Approximate location	*IP Address is collected and shared for location-based ad targeting and probabilistic attribution.* *Adjust and MAX SDKs do NOT request Android location permissions. However, if your application already has the relevant permissions and consent from the end user, location data can be used by MAX SDK. This feature is optional and can be disabled. See MAX documentation for more details.*	✓ Required	✓ Advertising or marketing ✓ Analytics	✓ Advertising or marketing ✓ Analytics
Personal Info	Email address	**Only applicable if you collect email address from user account creation or third-party SDK (Facebook Login)*		✓ App functionality ✓ Account management	✓ Advertising or marketing* **Only applicable if you have an email marketing program and use a third-party Email Service Provider (MailChimp, PostUp, Constant Contact, Unisender, etc)*
Financial Info	Purchase history	*For apps with In-app purchases*	✓ Required	✓ App functionality ✓ Fraud prevention, security, and compliance ✓ Personalization	✓ Advertising or marketing ✓ Analytics* **Only applicable if you use a third-party analytics tool for Payer Analysis or Payer Prediction (DeltaDNA, Firebase)*
App activity	Page views and taps in app Other actions	*Adjust and MAX SDKs collect app opens, session data.* *If SafeDK Ad Review is enabled, ads seen is also tracked.* *Most Adjust SDK integrations include other in-app events, which are shared with advertising*	✓ Required	✓ Analytics ✓ Advertising or marketing	✓ Advertising or marketing ✓ Developer communications * **Only applicable if you have an email marketing program that sends tailored content based on user's activity in the app.*

		networks for App Event Optimization.			
App info and performance	Crash logs Diagnostics		✓ Required	✓ App functionality ✓ Analytics	
Device or other identifiers	Device or other identifiers		✓ Required	✓ App functionality ✓ Analytics ✓ Fraud prevention, security, and compliance ✓ Personalization ✓ Account management	✓ Advertising or marketing ✓ Analytics* _*Only applicable if you use a third-party analytics tool for Payer Analysis or Payer Prediction (DeltaDNA, Firebase)_

Is this data processed ephemerally?

No

Definitions for your reference

App functionality – Used for features in your app. For example, to enable functionality, or authenticate users.

Analytics – Used to collect data about how users use your app, how your app performs. For example, to see how many users are using a particular feature, to monitor app health, to diagnose and fix bugs or crashes, or to make future performance improvements.

Developer communications – Used to send news or notifications about you or your app. For example, sending a push notification to inform users about an important security update.

Fraud prevention, security, and compliance – used for fraud prevention, security, or compliance with laws. For example, monitoring failed login attempts to identify possible fraudulent activity.

Advertising or marketing – used to display or target ads or marketing communications, or measure ad performance. For example, displaying ads in your app, sending push notifications to increase engagement, or sharing data with advertising partners.

Personalization – used to customize your app, such as showing recommended content or suggestions. For example, suggesting playlists based on users' listening habits, or delivering locals news based on a user's location.

Account management – Used for the setup and management of user accounts. For example, to enable users to create accounts, log in to your app, or verify their credentials.