An App Developer's Guide to GDPR

Konrad Kollnig

Version: 11th March 2021

No legal advice, only an app developer's attempt to make data protection more understandable.

If you have app users from the European Union, you are responsible for personal data collected through your app. Personal data is data relating to individuals. This may include device data, pseudonyms, user identifiers, advertising identifiers, (dynamic) IP addresses, and postcodes, especially in combination with other data. For these reasons, it is usually not possible to make personal data non-personal.

You are also responsible for personal data collected from your app for third-party services, such as advertising, analytics, or crash reporting services.

Risk evaluation and documentation. GDPR acknowledges that there will never be full protection of personal data. Instead, it encourages a risk-based approach, that is, seriously analysing the possible risks to data protection and taking appropriate data protection measures. If you can prove that you took all appropriate measures, there is no need to be overly afraid of high fines.

Make sure that you can provide such proof, by *documenting all data protection considerations, decisions, and actions.*

Reasonable data collection. You and your third-parties may only collect personal data reasonably, that is, only for the purposes stated in your privacy policy (purpose limitation) and restricted to what is necessary for the stated purposes (data minimisation).

Furthermore:

- *iOS:* According the Apple's terms, you should ask for user consent, before you or your third-parties collect *any data*, no matter if personal and non-personal.
  Android: According to Google's terms, if you process sensitive data (e.g. health-related), or process data in unexpected ways, do tell the user in a clear manner and ask for his *consent* (no pre-ticked boxes allowed).

- At best, use at most one third-party service for one purpose, that is, at most one advertising, analytics, and crash reporting service.

- Check with every app release, if you can reduce data collection or remove any third-party services.

- Verify the default settings of your third-party services (on-device and server-wise), since third-parties have an interest in collecting ever more data. Only activate third-party services, once user consent is established. More information can be found in the Appendix below.

- If your app is aimed at *children*, do not employ any third-party services. It's not good practice, and a violation of Apple's terms.

- If possible, use libraries that make their source code available. Otherwise, you have no means to verify the underlying data practices.

Always provide a privacy policy. Provide a privacy policy on the app store and within the app. You may want to use one of the privacy policy generators, such as `iubenda.com`. Make sure it discloses the data collection of you and your third-parties adequately.

Handling user requests. The GDPR entitles users to manage (e.g. access, delete, correct) any data about them. You can implement these user rights directly in software, which would show your efforts towards GDPR compliance. Yet, taking requests via email seriously is just as fine. You have one month to respond to user requests. This response may either address the request, or, for complex user requests, request an extension for a further 2 months.

Security measures and data breaches. Take the standard measures for security, such as HTTPS communications, salted passwords, validation of user inputs. Apple[1,2] and Google[3] provide comprehensive guidance on this. Try to remove identifiable information whenever possible, through pseudonymisation or anonymisation. If you experience a *personal data breach*, you must notify the data protection authority[4]

within 72 hours, plus the individuals in case of high risk.

Consent for third-party services. If you use third-party services, the user must be asked for consent in almost all circumstances. This consent must be sought before the third-party service is activated and begins to share data. Beyond consent, the Appendix provides more detail on the correct implementation of the most widely used third-party services.

Closing remarks. By implementing these measures, you should come an important step closer to compliance with GDPR. Additionally, you should consult the guidelines of an EU data protection authority. The British Data Protection Authority, called ICO, provides excellent guidance[5] on data protection.

[1] `https://developer.apple.com/documentation/security`

[2] `https://developer.apple.com/library/archive/documentation/Security/Conceptual/SecureCodingGuide`

[3] `https://developer.android.com/training/articles/security-tips`

[4] `https://edpb.europa.eu/about-edpb/board/members`

[5] `https://ico.org.uk/for-organisations/`

Appendix: Using Third-Party Services

Implementation guidance for the most commonly used third-party services, as well as links to their GDPR guidelines.

Service	Implementation Notes
Adjust	Once the Adjust SDK is enabled in your app, data sharing takes place, notably of device events. User consent should be established before enabling this SDK. It stands out that Adjust integrates the GDPR *right to deletion* into their SDK. This could be implemented in your app, to show your efforts to comply with GDPR. **More info:** `https://github.com/adjust/sdks`
AppLovin	For EU users, AppLovin requires consent to be passed on programmatically. If consent is given, the Advertising ID and IP address will be sent to advertising partners, otherwise only a country code. Once loaded at runtime, AppLovin automatically receives the information that the app was installed. **More info:** `https://www.applovin.com/gdprfaqs/`
AppsFlyer	The service collects the Advertising ID and a unique AppsFlyer user ID from the first app start. User consent should be established before activating this service. If the Advertising ID cannot be accessed, permanent identifiers, notably the device's IMEI, are shared with AppsFlyer, unless programmatically disabled. Such permanent identifiers are highly critical from a data protection standpoint. This practice should be communicated transparently to the user, if not disabled. **More info:** `https://support.appsflyer.com/hc/en-us/articles/360001422989`.

Facebook SDK	From the first app start, the Facebook SDK collects device information and events (app installation, app start, in-app purchases), unless programmatically disabled. User consent should be established before activating this SDK. Facebook serves no advertising, if the user limits interest-based ads from the device settings. **More info:** `https://developers.facebook.com/docs/app-events/best-practices/gdpr-compliance`
Flurry	For ads, this service provides a complicated mechanism to establish a user consent. Since legally required for many advertising services, you may want to consider easier, alternative approaches to establish valid user consent. Unless programmatically disabled, the user location is collected for analytics purposes, if the app has the permission to retrieve such. This is highly invasive and may violate GDPR. At very least, this practice should be disclosed to the user transparently, if not disabled. Generally, user consent should be established before activating this service. **More info (Analytics):** `https://developer.yahoo.com/flurry/docs/analytics/gdpr/summary` **More info (Ads):** `https://developer.yahoo.com/flurry/docs/publisher/gdpr/`
Google AdMob	This service serves personalised advertising by default, violating Google's policies if used in the EU. This must be changed by the developer, such that user consent is established prior to serving personalised ads. AdMob shares device statistics and events with Google from the first app start, unless programmatically changed. User consent should be established before activating this service. **More info:** `https://developers.google.com/admob/android/eu-consent#forward_consent_to_the_google_mobile_ads_sdk`.

Google Analytics	User opt-out and IP anonymisation are supported programmatically and their implementation should be considered. User consent should be established before using this service. **More info:** `https://developers.google.com/analytics/devguides/collection/android/v4/advanced`
Google Crashlytics	This service shares crash reports with Google from the first app start, unless changed by the developer. User consent should be established before activating this service. **More info:** `https://firebase.google.com/docs/crashlytics/customize-crash-reports#enable_opt-in_reporting`
Google DoubleClick	This service serves personalised advertising by default, violating Google's policies if used in the EU. User consent should be established before activating this service. **More info:** `https://developers.google.com/ad-manager/mobile-ads-sdk/android/eu-consent#forward_consent_to_the_google_mobile_ads_sdk`.
Google Firebase Analytics	This service collects device statistics from the first app start, unless changed by the developer. The collected data includes the Google Advertising ID, unless programmatically disabled, and may be used for advertising purposes under certain circumstances. User consent should be established before activating this service. **More info:** `https://firebase.google.com/docs/analytics/configure-data-collection`
Inmobi	The Inmobi SDK only collects personal data, if you explicitly indicate to the SDK that user consent was established. If no consent is given, unpersonalised ads are shown to the user. Inmobi encourages you to provide data about location and demographics for higher revenue, if you programmatically pass on this information. Such sensitive data collection should be transparently disclosed to the user, if not refrained from. **More info:** `https://support.inmobi.com/monetize/faqs/gdpr-guide-for-publishers/`

MoPub	For increased advertising revenue, MoPub shares data with two other services, IAS and Moat, unless programmatically disabled. These services must be transparently communicated to the user, if not disabled. User consent should be established before activating this service. **More info:** `https://developers.mopub.com/publishers/best-practices/gdpr-guide/`
Unity Ads	Unity automatically asks for user consent, unless a special arrangement is reached with Unity. Personal data is only collected if the user consents. When ads are served, Unity provides the user with a 'privacy icon', to change his opt-out setting. If the user opts-out, all collected data is deleted. **More info:** `https://unity3d.com/de/legal/gdpr`