**GDPR Process for Mobile Applications**

Table of Contents

[**GDPR Definitions** 3](#_Toc45289738)

[**Does the GDPR affect me?** 3](#_Toc45289739)

[**What is “Personal Data”?** 3](#_Toc45289740)

[**What does the GDPR mean for your mobile app?** 3](#_Toc45289741)

[1. **Privacy by Design** 4](#_Toc45289742)

[**2. Ask for Explicit Consent** 5](#_Toc45289743)

[3. **Providing Visibility and Transparency** 5](#_Toc45289744)

[**4. Respond to User Requests** 6](#_Toc45289745)

[**5. The Right to Be Forgotten** 6](#_Toc45289746)

[**6. Review services and SDKs you use** 7](#_Toc45289747)

[**7. Data Breach Notifications** 8](#_Toc45289748)

[**8. Encryption and data storage** 8](#_Toc45289749)

[**9. Log and Justify Your Data Collection** 8](#_Toc45289750)

**GDPR Definitions**

Data Controller: A Data Controller is the entity that determines the purposes for and means of collecting and processing personal data. If you own a website or mobile app, and you’re deciding what is collected, how it is collected, and for what purpose, you are a Data Controller.

Data Processor: A Data Processor is an organization that processes personal data on behalf of a data controller.

Data subject: a natural person whose data is processed. For example, an app user or a website visitor.

**Does the GDPR affect me?**

Most likely, yes!

The GDPR applies to all businesses with customers, or website/mobile app visitors who are from the European Union (EU). This means that any organization in the world that works with EU residents’ personal data in any manner has obligations to protect their users’ data and be GDPR compliant.

**What is “Personal Data”?**

“*Personal Data*” under the GDPR includes any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

The scope of this is broad, and includes anything from personal information, to a cookie placed on someone’s browser by an analytics tracking tool you might use to track your website usage.

**What does the GDPR mean for your mobile app?**

The fines for not being GDPR compliant are high – either 4% of annual global turnover or €20 million (whichever is greater!).

With GDPR compliance becoming a requirement for every business with either customers or website visitors, or app users in the EU, you’re probably concerned about whether or not your mobile app is GDPR compliant.

As a mobile app publisher, you will need to understand how you obtain, transfer, store, and handle your user data. You should take some time to understand exactly how you currently ensure data security for your users, and what you can do to improve this in order to have a GDPR compliant mobile app.

[Cennydd Bowles sums up](https://medium.com/@cennydd/a-techies-rough-guide-to-gdpr-c8d4b4eb2b3b) why you should be compliant, even if it may be a lot of work initially:*“You may end up with less rich customer insights than you had before. Some KPIs may slump. But for companies that have direct customer relationships, it’s all manageable, and on the upside you not only reduce your compliance risk but benefit from the increased trust your customers will show in you and the online world in general.”*

Below are some key highlights that are relevant to your mobile app and business in general that will help you ensure GDPR compliance.

1. **Privacy by Design**

Privacy by Design is now a legal requirement under the GDPR. From the moment you start creating your mobile app, you should be considering your users’ privacy.

When you’re developing your mobile app, or having a third party develop it, you need to consider data protection and user privacy.

Privacy by Design is not a new concept and pertains to thinking of your users data privacy in your app, website, or software from the very start, rather than leaving it as an afterthought. The idea of privacy by design includes deciding what data you need, and what data you don’t. In [Brian Pagan’s overview to designing apps with privacy in mind](https://brianpagan.net/2018/privacy-a-quick-overview-for-app-designers/), he asks if you really need a users name AND date of birth. In many cases, just one of these fields is enough. He writes:*“the risk of someone opening a credit card in my name far outweighs the benefit of getting that “happy birthday”  marketing e-mail from your company.”*

**Recommendation:**

Think about your user data from the very start, and don’t let it be an afterthought.

You should be thinking about Privacy By Design when you’re creating new features, or creating a new page on your app in order to remain GDPR compliant.

As well as this, you should encrypt personal data with strong encryption algorithms. This will help you minimise the impact of a data breach.

**2. Ask for Explicit Consent**

Under the GDPR, businesses must request and receive user consent in order to collect, use, and move personal data.

This includes data collected for advertising, [analytics](https://www.mobiloud.com/blog/wordpress-analytics/), crash logging or anything else. The opt-in must be understandable and clear.

Explicit Consent can be granted easily through an opt-in screen when your app launches. Your app users chose to download your app in the first place, so the likelihood is, most people will be happy to grant consent in order to use your app and receive further communications from your business, provided the recipient can see a benefit.

Your users must also be able to withdraw consent as easily as they are able to give it. You may need to update your Privacy Policy to address this, and add another page on your website where users can opt-out.

**Recommendation:**

When someone registers on your mobile app, they should be asked to opt-in to have their data collected, or to receive communications, such as emails or Push Notifications. We highly recommend showing a consent screen on app launch, as this is the only way to be fully GDPR compliant. You should also notify users on these screens exactly where their data will be used. For example, will they be tracked in Google Analytics, or have data sent to Google Admob to show them relevant ads? Your users need to know, and it’s your obligation to inform them as soon as they begin using your GDPR compliant mobile app!

As well as this, your GDPR compliant mobile app should have a dedicated page where users can opt out of communications from you, or ask for their data to be removed from them.

3. **Providing Visibility and Transparency**

One of the most important aspects of GDPR is how the data you collect is actually used. If you are a data controller, you need to be aware of how your users can effectively manage, and protect their user data.

Proving visibility and transparency through a clear, and understandable Privacy Policy not only benefits the users of your mobile app, but it’s a requirement from the App Stores. Google will remove your app if they can’t find a Privacy Policy on your Play Store’s profile page and accessible inside your app.

You should also provide information to your users over which third parties you are using to collect or process user data.

For example, if your app connects to external services such as user analytics solutions (e.g. Google Analytics, Fabric), advertising providers (e.g. Admob, MoPub), or push notification providers (e.g. Firebase, OneSignal), you should disclose this to users clearly in your Privacy Policy.

You should also make sure that all third-party providers which collect any user data are GDPR compliant. They’ll be “data processors”, while you remain the “data controller”. As such you should have written agreements in place which meet the level of assurances in terms of data protection and security which GDPR requires. For some of them, you’ll be able to sign data processing agreements which add the required wording to the existing terms of your agreement.

**Recommendation:**

Create or update your app’s Privacy Policy page for your mobile app. You may choose to have a Sidebar or Menu item that links to the legal terms of your mobile app. This will enable users to easily find, read, and understand how your mobile app is using their data.

**4. Respond to User Requests**

If someone asks how you are using their data, under GDPR you are legally obligated to respond to them. This is called a  Subject Access Request.  
A Subject Access Request may be done physically, or digitally. When a user asks for information about their data or a copy of their data that is used in your mobile app, you have one month to respond. For complicated requests, you will have up to three months to respond.

**Recommendation:**

Create a page on both your website and mobile app that includes your business contact information. This will allow users to contact you easily, and provide transparency from your side. Make an effort to respond quickly and clearly to all Subject Access Requests.

**5. The Right to Be Forgotten**

When a user asks you to remove their data acquired through your website or mobile app, you are obligated to remove every personal detail you hold about them in all systems, whether you control their data directly or through a tool or SaaS you use in your app (for example, Google Analytics).

If you want your mobile app to be GDPR compliant, you could choose to provide solutions such as deleting user data from your own database directly from the app, or having a simple contact form or dedicated page where a user can request their data to be erased.

**Recommendation*:***

Be transparent and allow users to easily contact you about erasing their data. When someone asks for their data to be erased, take the request seriously and comply with the request on every system you control.

You are also obligated to notify Third Party Data Processors that the data must be deleted from their servers too. This can be done through calling an API of theirs that allows for the deletion of personal data (if this is made available by the provider).

**6. Review services and SDKs you use**

If your app sends personal data to an external service for processing (e.g. to analyse app usage), you need to be clear and transparent about where this is, and who will be in control of the transferred data.

It is the responsibility of the data controller, in this case, you, the app publisher, to ensure that all Third Party data processes are GDPR compliant, and have appropriate data security measures in place. To ensure this, you should talk to your third party partners directly, ask them about their latest Privacy Policy and Terms and what they’re doing for GDPR compliance.

It’s worth the time it takes –

Marcus Turner, CTO of [Enola Labs](https://www.enolalabs.com/) says that, “*Ultimately, higher levels of cyber security are a necessary and worthwhile investment for business owners that care about protecting their customers and safeguarding their business. I often tell businesses that they can pay an upfront cost now to protect their data, or wait until a cyber security attack and pay an even bigger price later to clean up the mess. Waiting may very well cost you your business*“.

So, make sure you take the time to review your technology suppliers and invest in necessary ones that will help safeguard your business from being in breach of the GDPR.

**Recommendation:**

You should only have contracts with providers who can provide ‘sufficient guarantee’s that GDPR requirements will be met, and your users’ data is sufficiently protected.

Many vendors will have GDPR pages on their website, or have updated their Privacy Policy or Terms and Conditions to ensure GDPR compliance. You should familiarize yourself with this, or talk to someone from their support or legal team to understand if they are GDPR compliant or not.

**7. Data Breach Notifications**

To increase trust between customers and businesses, and in the wake of [notable data breaches](https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html) from companies the GDPR is enforcing tighter deadlines for businesses to notify national supervisory authorities and their users. Disclosure must happen within 72 hours.

**Recommendation:**

Establish a clear step by step process that you can use in case of a data breach that includes how you will inform users and national supervisory authorities of the breach.

**8. Encryption and data storage**

Your mobile application should use [SSL](https://info.ssl.com/article.aspx?id=10241) or [HTTPS](https://www.instantssl.com/ssl-certificate-products/https.html) for external communications. When communicating personal information of any kind, that data must be encrypted. Not encrypting data means that information sent will be in clear text and will be exposed over the internet.

If you built an app that connects to your website or web servers and transmits sensitive data (e.g. a username/password), you should verify that you’re using SSL for all connections from your app.

Encryption is not only relevant for external communications. All data that your mobile app collects should be stored in a safe place and, and your backups should also be encrypted. Users should also know how long their data will be retained for.

**Recommendation:**

Ensure that your app uses secure communications through SSL and HTTPs, and make sure your SSL certificate has been properly deployed.

All data stored should use encryption, and you should provide transparency to data subjects over how long you retain this data for.

**9. Log and Justify Your Data Collection**

[Article 30](https://gdpr-info.eu/art-30-gdpr/) of the GDPR outlines that each data controller, or representative of the controller, *“shall maintain a record of processing activities under its responsibility”*

This means that in order to ensure your GDPR compliance, you should start documenting all the data that you collect (either yourself, or through a third party).

You should create a secure, comprehensive log of your data collection activities.

This log should include all and any kind of personal data that you are collecting on website visitors and users. From people’s names (if collected) to IP addresses to the country they’re located in.

Then, you should justify *why*you’re collecting this data. You need to identify *where*you’re storing it, how long it is stored for, *how*can the data collection be justified, and more.

**Recommendation:**

Make sure you’re fully aware of every kind of user data that you’re collecting and ensure you can justify why you’re collecting it.

Clear, complete documentation that you can refer back to will not only help you when customers or users ask about your GDPR policies but ensure regulatory compliance and safeguard both your business and mobile app.