

Game Developers Watch Out! German Data Protection Authorities Publish Guidelines for Mobile Apps



In a joint effort, a working group reuniting all German Data Protection Authorities ("DPAs") has now published its long-awaited guidelines for developers of mobile games and apps. The 33 page document defines legal requirements for apps and also addresses the underlying technical framework.

The end of the ceasefire

The document does not really contain any surprises, but it is still a useful and interesting read, because for the first time ever the regulators are letting us know how they believe data privacy legislation should be interpreted for mobile games and other apps. And anyone commercializing apps in Germany would be well advised to heed these rules of the game: The DPAs have announced that they will now get down to business with non-compliant apps.

The regulators had conducted "app sweep days" before to examine apps with regard to their legal compliance. Among the recurring grievances was a lack of clarity as to what data are collected by the apps and for what purpose they are used and shared. However, until now the DPAs had only followed up with actual enforcement action in exceptional cases.

Disregarding the new guidelines can carry fines of up to EUR 300,000 and lead to considerable brand damage. We are already seeing increased activity from the DPAs, but also from consumer protection watchdog groups. The days of the legal ceasefire are over.

Guidance in a nutshell

In a nutshell and amongst many other points, the guidelines require app developers to comply with the following:

- During the development process, app developers must ensure that only such personal user data is collected and processed as is absolutely necessary for the performance of the app.
- Users have to be informed about the type, scope and objective of the collection, the processing and the use-cases of their personal data in a comprehensible manner. This requires an app-specific privacy policy.

- The privacy policy should ideally be integrated into the product page in the respective app store so that users can take note of it before the download. It is insufficient to use a privacy policy designed for a similar web service.
- The privacy policy must specifically address the data collection and use via the app. For instance, any collection of data via the various sensors of a mobile device, like the camera or the microphone, must be disclosed, along with any mobile tracking technologies.
- The privacy policy and the developer's contact information must be integrated into the app and be easily accessible from within the app.
- The principle of "Privacy by Design" is a leitmotiv of the guidance paper – app developers need to build their product with privacy requirements in mind from the outset, and integrate privacy mechanisms into their design.
- Specific requirements apply to location data, generally considered as particularly sensitive. Thus, the guidelines require not only transparency but also reducing the granularity of such data to the extent possible.
- Similarly, stricter rules apply with regard to health, banking data and other sensitive personal data, including data of minors. Finally, the guidelines set forth a number of technical safeguards that app developers are required to implement (again: privacy by design), including sufficient server backend encryption, secure password requirements, etc.

Why this matters to international businesses

German data protection law applies not only to businesses based in Germany. It also applies to any data collection processes within Germany (for example by an app installed on a German user's smartphone) controlled by an entity outside the European Union.

Even though as a general rule, entities within the European Union only need to adhere to their own member state's privacy law when doing business across the EU, recent ECJ case law suggests that a consumer's local privacy laws may even apply in many cases when data collection

Game Developers Watch Out! German Data Protection Authorities Publish Guidelines for Mobile Apps



processes are controlled by an EU entity that has an affiliate or branch office in such consumer's jurisdiction.

The DPAs primarily regard the providers (developers and operators) of mobile games and other apps responsible for complying with privacy rules. Therefore, the paper is primarily targeted at such app providers, while making it clear that also other parties, including the app stores, bear a certain responsibility under data privacy laws.

Anyone involved in the mobile games business should therefore now make sure their apps are compliant – before the regulators do.

*This article is current as of the date of its publication and does not necessarily reflect the present state of the law or relevant regulation.



Konstantin Ewald
Head of Digital Business, Germany
Partner/Rechtsanwalt
Innere Kanalstr. 15 50823 Cologne
T +49 (0) 221 5108 4160
E konstantin.ewald@osborneclarke.com



Felix Hilgert, LL.M.
Associate
Innere Kanalstr. 15 50823 Cologne
T +49 (0) 221 5108 4160
E felix.hilgert@osborneclarke.com