6.3.2023

EGDF position on the implementation of the DMA

1. About EGDF

1. **The European Games Developer Federation e.f. (EGDF)**[1] unites 23 national trade associations representing game developer studios based in 22 European countries: Austria (PGDA), Belgium (FLEGA), Croatia (CGDA), Czechia (GDACZ), Denmark (Producentforeningen), Finland (Suomen pelinkehittäjät), France (SNJV), Germany (GAME), Italy (IIDEA), Lithuania (LZKA), Netherlands (DGA), Norway (Produsentforeningen), Poland (PGA and IGFP), Romania (RGDA), Serbia (SGA), Spain (DEV), Sweden (Spelplan-ASGD), Switzerland (SGDA), Slovakia (SGDA), Portugal (APVP), Turkey (TOGED) and the United Kingdom (TIGA). Through its members, EGDF represents more than 2 500 game developer studios, most of them SMEs, employing more than 45 000 people.

2. **The games industry** represents one of Europe's most compelling economic success stories, relying on a strong IP framework, and is a rapidly growing segment of the creative industries. The global Android and iOS app consumer spending was $129 billion in 2022, and games accounted for 67% of that revenue[2]. The European digital single market is the third-largest video game market globally. All in all, Europe's video games market was worth €23bn, and the industry has registered a growth rate of 22% over 2020 in key European markets[3]. There are around 4 600 game developer studios and publishers in the EU, employing over 74 000 people and running a combined turnover of more than €16,6bn in 2020[4].

3. **The European Commission and EU member states must carefully balance**: 1) the measures to protect players from fraudulent behaviour on existing and future application store platforms; and 2) actions to secure free and fair competition in the platform economy.

[1] For more information, please visit www.egdf.eu
[2] https://www.businessofapps.com/data/app-revenues/
[3] ISFE-EGDF 2021 Key Facts
https://www.isfe.eu/wp-content/uploads/2022/08/FINAL-ISFE-EGDFKey-Facts-from-2021-about-Europe-video-games-sector-web.pdf
[4] EGDF-ISFE 2020 European games industry insights report
https://www.egdf.eu/wp-content/uploads/2022/09/ISFE_EGDF-report2022_V08-05092022_45FIXED.pdf

2. Direct downloading

4. **What is direct downloading (sideloading)?** In the mobile app ecosystem, direct downloading means downloading apps outside the Apple Appstore or Google PlayStore. Direct downloading is already possible on Google Android OS but it is not an encouraged practice, as Google enforces excessive and unnecessarily alarming warnings and cumbersome download flow. On Apple IOS, direct downloading requires jailbreaking the whole device, which is against Apple's Terms of Service and far beyond the skill sets of an average player.

5. **Opportunities of direct downloading for game developers – less censorship and more competition and growth**

    a. Currently, Apple is well known for censoring games from its application stores. In practice, this means that Apple is actively blocking any content that it finds to be "poor taste"[5], particularly games that explore ways of expressing human sexuality. DMA will force Apple to allow alternative application stores on its platform, significantly strengthening the artistic freedom of European game developers who are no longer forced to follow non-European content policies. When DMA allows game developers to bypass Apple's 30% payment commission, new mobile application stores will be able to compete with lower prices or use the extra financial resources to compete with better or more risk-taking content.

    b. SidequestVR[6], which allows direct downloading for the Oculus VR platform, is an excellent example of a direct downloading platform that strengthens experimentation and risk-taking by providing a route for experimental games, early demos and test versions, and ports of existing games from other platforms to enter a walled VR garden.

6. **Risks are associated with direct downloading – players must be protected**

    a. The security of the players is among the key priorities of European game developers. Securing that games are distributed through trusted and secure distribution channels is crucial for building player trust. For example, this player trust exists with several of the game stores available on PCs. These stores prove that direct downloading can be accomplished safely from trusted sources. Compared with other platforms, smart mobile devices are somewhat different in that they can collect a lot of sensitive data on their users (e.g. health data and location data) and are widely used for two-factor authentication of users. It is, therefore, crucial to take measures to prevent DMA from being misused for fraudulent or harmful behaviour.

    b. The risks of fraudulent applications are not exclusive to direct downloading. Already now, especially on Android, both the official Google Play store and direct downloading are misused to mislead players into downloading fraudulent applications. Fraudulent apps persistently pop up also within Apple's App Store as well. Sometimes these applications are copycat games misleading players to believe that they are created by well-known and trusted European game developers and sometimes clearly pirated versions of European games.

[5] https://developer.apple.com/app-store/review/guidelines/
[6] https://sidequestvr.com/

c. Apple Appstore and Google Playstore set high standards on player safety and security, and we hope that by opening up competition in mobile app distribution, the DMA will create a "race to the top" on safety and security among all app distributors.

7. **Apple and Google must not be allowed to kill the emerging third-party application stores with alternative fees**

a. Already now, the number of Apps, for example, payments for food, physical products, and tangible services, bypass the 30% commission[7]. In practice, this means that Apple does not take a cut of consumer's money, for example, for Starbucks mobile orders, Etsy products, or Uber rides. Meanwhile, in 2022 in a Dutch antitrust case, Apple proposed a 27% commission on all third-party payments for a Dutch dating app[8].

b. Most likely, the first third-party application stores will be launched by big global industry giants. At the moment, almost all European actors are waiting for more legal certainty on how the DMA is implemented, in particular, if alternative platform fees are allowed, before taking the financial risk of investing in their own third-party distribution channels.

c. The Commission should carefully investigate when alternative fees, for example, should be considered anticircumvention behaviour (DMA Art.13) and when they violate fair, reasonable and non-discriminatory general conditions (DMA Art. 6 (12). If Apple and Google are allowed to introduce alternative fees and other conditions of access to their platforms, these fees and conditions must be the same, reasonable, non-discriminatory, and fair for all apps and content. Apple and Google must not be allowed to abuse their dominant market position to kill emerging third-party markets with almost 30% alternative fees that would make it financially unsustainable to launch any third-party application store.

8. **How to balance risks brought by direct downloading with the competition benefits introduced by DMA?**

a. According to DMA Art. 6 (4), the measures protecting the integrity of the hardware or operating system must be **duly justified**, **strictly necessary** and **proportionate**. Recital 50 clarifies that the gatekeeper should always choose the **least restrictive** measures.

b. **We need measures that are strictly focused and limited.** The actions taken to protect the app ecosystem should be strictly limited to necessary and justified legal compliance, trust, privacy, security and safety measures. **The following actions can not be considered necessary, justified and proportionate:**

i. **Censorship:** Protecting the integrity of the app ecosystem should not be used as an excuse for censorship. Gatekeepers should not be allowed to block access to application stores that allow content they consider "poor taste" by non-European standards.

ii. **Blocking innovation:** Protecting the integrity of the app ecosystem should not be used as an excuse for blocking business and technological innovation in Europe. In

[7]https://www.insightpartners.com/ideas/do-you-have-to-pay-the-apple-tax-its-complicated/

[8] https://www.theverge.com/2022/2/4/22917582/apple-netherlands-antitrust-27-percent-commission-alternative-in-app-payment-systems

2016, for example, Apple banned all crypto-mining apps and exchanges, not just the ones that did not fulfil European regulatory requirements[9].

iii. **Blocking competing products:** The protection of the integrity of the app ecosystem should not be used as an excuse for blocking competing applications. Apple has for years blocked all mobile cloud gaming platforms and game subscription services competing with its AppleArcade service from its application store.

iv. **Blocking European standards or self/co-regulatory actions:** Apple, for example, does not allow game developers to use European co-regulatory PEGI age rating to protect minors. Instead, they force game developers to use their own Apple age rating system that does not allow European game developers to follow European legal standards. For example, the maximum Apple age rating is an "over 17" rating, whereas some EU member states would require an "over 18" age rating.

v. **Blocking in-app communication and marketing features:** As required under DMA art. 5(4), gatekeepers must not be allowed to block directly downloaded apps from using or communicating with their users about an option to use third-party payment systems.

c. We need fair competition based on trust – trusted third-party application stores as a solution

i. **Third-party distribution channels by trusted third parties are nothing new:** Already now, the Apple Developer Enterprise Program[10], for example, allows large organisations to develop and deploy proprietary, internal-use apps to their employees.

ii. **Apple and Google should create specific programs for trusted third-party application stores** that commit to high-security standards, following European platform, consumer and privacy rules, taking down fraudulent apps (e.g. copycat games), taking down games violating copyrights, etc. Effective use of third-party application stores means that downloading apps from trusted application stores should follow exactly the same procedure as those downloaded from Apple Appstore or Google Playstore.

iii. **Only apps that are directly downloaded from the web should receive extra security prompts.** Those prompts should be reasonable and proportional and provide information that enables the consumer to determine whether they trust the publisher. The prompts should not be so numerous as to make it inconvenient for users to directly install software that they trust nor should the prompts deploy language intended to scare users or inaccurately suggest that installing an application is dangerous.

iv. **As stated in the DMA art. 6 (7), the trusted third-party application stores should have access to and be interoperable with the same operating system-level features as the Apple Appstore or Google Playstore.** These

[9] https://www.theverge.com/2018/6/11/17449178/apple-app-store-cryptocurrency-mining-ban-ios-macos
[10] https://developer.apple.com/programs/enterprise/

features include, for example, parental control tools and player's subscription management tools.

d. We need measures that are strictly focused and limited – minimum mandatory safety and security measures

i. **In order to be able to install directly downloaded apps, it is justifiable and proportionate, for trust, privacy, security and safety reasons, to demand that all developers verify that they are who they claim to be and scan the apps for malware.**

ii. Gatekeepers must not be allowed to misuse a developer installer certificate or any other developer account to delay or block access to their platforms. Furthermore, it is important to secure that gatekeepers do not use trust, privacy and security concerns to introduce new market access barriers (e.g. new fees). Therefore, developer identification and malware detection process should be free of charge and used only to identify an app developer so that fraudulent or unlawful applications can be taken down on the operating system level.

9. **The Commission must provide solid implementing regulations and clear guidelines so that European stakeholders will be able to explore their new rights in the mobile application market**s**.** Furthermore**,** the Commission should provide further guidance on third-party application stores by other gatekeepers.

3. Alternative web browser engines and DMA

10. **At the moment, the most common web browser engines, WebKit (Apple), Blink (Google, Microsoft, Meta) and Gecko (Mozilla), provide more or less the same features for game developers.** There has been little investment into alternative mobile browsers because of mandates by mobile operating system gatekeepers that prohibit equal access: to processing power, hardware, OS APIs and other features necessary to build successful games. These restrictions have been harmful to players and game developers and have circumscribed innovation in alternative browsers.

For more information, please contact,

Jari-Pekka Kaleva
Managing Director, EGDF
jari-pekka.kaleva@egdf.eu
www.egdf.eu