Submission of additional information

Compliance measures with the Digital Markets Act proposed by Apple Inc.

The undersigned civil society organisations and stakeholders affected by DMA measures would like to thank the European Commission's DMA enforcement team for the series of compliance workshops with gatekeepers organised in March of 2024.

Following up on the sometimes rushed conversations that occurred there, we find it useful to provide the additional context, legal arguments, and data below for the Commission's consideration, and hope that this information might also contribute to the ongoing non-compliance investigations, including the one newly announced at the ECN DMA Conference this week. Moreover, we applaud the Commission for swiftly producing the preliminary findings confirming that Apple's App Store rules are in breach of the DMA "as they prevent app developers from freely steering consumers to alternative channels for offers and content."[1] Finally, we prompt the Commission to adopt non-compliance decisions against Apple as swiftly as possible and to impose the relevant fines. We are also particularly encouraged by Vice-President Margrethe Vestager's remarks during the aforementioned conference that there are "no reservations about proceeding to structural remedies."

App stores and sideloading

The app choice provision of Article 6(4) is one of the DMA's key means for enabling competition and user choice in the gatekeepers' respective app ecosystems. Apple has presented a compliance plan regarding its App Store that can only be interpreted as an attempt to circumvent this DMA provision's goal. Concretely, paragraph 4 obliges the gatekeeper to provide users with the possibility to easily install apps from other sources than the gatekeeper's own software application store. Recital (41) clarifies that the gatekeeper is prohibited from undermining or restricting that possibility in any way.

1 Commission sends preliminary findings to Apple and opens additional non-compliance investigation against Apple under the Digital Markets Act, Press Release, 24 June 2024.

Yet, as part of its compliance measures, Apple proposes that app developers who wish to break free from the gatekeeper's dominant app store service will still have to subscribe to and pay a so-called "Core Technology Fee" (CTF) for a mandatory "notarisation" service controlled by the gatekeeper. In addition to the CTF, an aspiring marketplace creator who does not already have a very popular app in the gatekeeper's App Store must provide an annual 1 million euro letter of credit in order to be approved for the marketplace entitlement. In **blatant disregard to the DMA's objective** to ensure contestable and fair digital markets, Apple argues that its app store competitors should first have to be "authorised" by the gatekeeper itself before being able to compete with it. And the financial barriers that it has erected – which it may increase to arbitrarily high amounts at any time – ensure that all but the most well-funded commercial vendors are excluded from running an app store and competing with the gatekeeper.

Apple claims that its mandatory notarisation "provides some check to ensure that apps are free of known malware, viruses, or other security threats, function as promised, and don't expose users to egregious fraud,"[2] but as was pointed out by participants of the respective compliance workshop, the company has provided no evidence that other app store providers or even third party notarisation services cannot provide the same or a higher level of protection from such threats.

Apple also claims that its own forced and billable notarisation service was necessary because app distribution through channels other than those from Apple risks compromising the devices "system integrity". The DMA allows gatekeepers to take "strictly necessary and proportionate measures" to ensure the "integrity of the hardware or operating system". The Oxford Dictionary defines integrity as "the state of being whole and not divided." Recital 50 clarifies that for any restrictive measures, the gatekeeper must demonstrate "that such measures are necessary and justified and that there are no less-restrictive means to safeguard the integrity of the hardware or operating system."

In this context, it is crucial to note Apple's own rules for its other products: The company does not impose any notarisation requirement or fee for its own macOS operating system, on which developers can sell their apps directly to users without interference from the gatekeeper, and—most importantly—without any negative impact for the "system integrity" of Apple computers running macOS. That is because installing apps from other sources without mandatory gatekeeper notarisation **does not endanger the integrity of the hardware of operating system**.

What is more, Apple itself offers sideloadable apps from outside any app store for other operating systems: The gatekeeper notably promotes its own Apple Music app for Android to download from their website[3] and thereby not only encourages Android users to sideload apps—a practice that Apple misleadingly claimed threatens device integrity—but it also circumvents their competitor's own app store offer. It becomes clear that Apple's forced "notarisation" system has nothing to do with user safety or device integrity but has everything to do with gatekeeper control and monopoly rent seeking.

2 Apple, *Apple's Non-Confidential Summary of DMA Compliance Report*, 7 March 2024, page 3. It is unclear from Apple's compliance report whether that means the company would allow non-egregious fraud in its notarisation process.

3 Apple Music for Android is available as APK file at https://apple.com/lae/apple-music/android-download, last accessed on 29 May 2024.

As broadly as Apple might want to interpret the meaning of paragraph 4's integrity exemption, it can hardly be argued that people's iPhones or even iOS will fall apart just because Apple cannot vet and vouch for every single app that any of the 2 billion+ people owning an iOS device[4] installs.

Apple's compliance proposal—and any mandatory app authorisation process imposed by the gatekeeper—is therefore **infringing Article 6(4) DMA**.

The attempt to force all app developers who wish to distribute their apps independently from Apple to use and pay for the gatekeeper's own notarisation service is not only incompatible with Article 6(4) but also a **breach of Article 13(6) DMA**, the anti-circumvention provision. Firstly, Apple's proposed compliance solution seriously degrades the conditions under which app developers can distribute their apps to iOS users as well as the quality of service for iOS users who wish to install their apps from sources not controlled by the gatekeeper. Secondly, it makes the exercise of those rights unduly difficult, in particular by subverting the end users' and the app developers' autonomy to interact with each other without interference by or knowledge from the gatekeeper. Lastly, as mentioned above, Apple's proposal is entirely incompatible with industry standards applied to all other major operating systems on the market, including macOS, Windows OS, Android, Sailfish OS, Ubuntu Touch and professional Linux distributions, where the autonomous distribution and installation of apps is naturally possible.[5] [6]

Apple's compliance proposal is also **in breach of Article 5(4) DMA**, which obliges the gatekeeper to allow business users to conclude contracts with end users, including contracts about the provision of smartphone apps, *regardless of* whether they use the core platform services of the gatekeeper to conclude those contracts. Forcing app developers to run their products and services by the gatekeeper for authorisation or "notarisation" as proposed by Apple is fundamentally incompatible with this anti-steering clause. That is why this infringement of the DMA is not caused by the amount of fees Apple charges, as it is a question of the gatekeeper retaining undue and full control over business users' and competitors' commercial opportunities as well as the end users' freedom to run software on the devices they own.

With its compliance proposal, Apple tries to repeat the same monopolistic behaviour it has applied to browser engines for years: namely that vendors are permitted to provide an alternative user interface to Apple's gatekeeper service (then the browser engine, now app notarisation) but not to offer real competition to Apple's core service and source of market dominance. This kind of behaviour has been explicitly outlawed for browsers by Article 5(7) DMA and it also circumvents Article 6(4) with regard to software application stores.

---

4 Umar Shakir, *Apple surpasses 2 billion active devices*, The Verge, 2 February 2023.

5 Apple's macOS includes notarisation controls by default but they can be ignored by developers by cryptographically signing their app, and they can be overridden by end users for software that is otherwise trusted. Also see Apple, *Safely open apps on your Mac*, available at https://support.apple.com/en-us/102445, last accessed 13 June 2024.

6 In its Windows operating system, Microsoft offers a service called "Smart App Control" which, according to the company offers an "intelligent cloud-powered security service can make a confident prediction about its safety". This system is *not* a notarisation process and it can be easily deactivated by end users. Like on Apple's macOS, Windows users are free to choose which software they wish to run on their devices without interference by the gatekeeper.

Choice screens

We welcome the fact that Apple has chosen to integrate the browser choice screen prescribed by Article 6(3) DMA directly into the Safari browser. It also is appropriate that this choice screen is only shown to users who have set Safari as default browser or have not selected a default browser yet.

However, if Apple truly aims to provide users with the "best possible experience", as the company claimed during the compliance workshop of 18 March 2024, it is crucial that its **compliance with Article 6(3)** works hand in hand with the app store requirements of paragraph 4, i.e. that the default browser selected by a user is directly installed from the default app store, without additional user interface friction that might confuse users or scare them away from their choice. Such extra friction is what researcher call "roundabout", or an interface "designed to tire or bore a decision-maker, or otherwise redirect a decision-maker when they are trying to achieve an outcome."[7] It is a well-studied pattern of manipulative interface design built to discourage end users to take a consumer decision that conflicts with the gatekeeper's commercial interests.

Also, Article 6(3)'s default browser provision will fail to have its intended effect, if the default browser is not being used due to its icon being hidden on screen 4 of the user's mobile device. That is why a newly selected default browser's icon should always automatically replace Safari's preferential ranking on the home screen's 'hot seat', i.e. the bottom row of most used app icons that is always visible to users across screens. Otherwise, Apple's own Safari will continue to enjoy its pre-installed preferential position on users' screens and undermine its effective compliance with the obligations under Article 6(3) as well as make it unduly difficult for users to replace Apple's Safari browser with another default, including on their home screen. Keeping Safari in this preferential spot despite a user's explicit choice for another default browser therefore also risks **infringing the anti-circumvention clauses of Article 13(4) and (6)**.

Allowing end users to "easily change default settings" such as the default browser as prescribed by Article 6(3), the provision must also be interpreted to include an obligation for the gatekeeper to allow third party browsers to prompt users on first launch with an option to make that browser the default. Otherwise, users who already know which other browser they would like to use, and have installed it themselves, would have to counter-intuitively open the gatekeeper browser first in order to trigger the choice screen. Such an in-browser prompt is in line with long established industry standards on desktop platforms like Apple's own macOS and Microsoft Windows OS, as well as with the **sister provision of Article 6(4)** which mandates the gatekeeper to "not prevent the downloaded third-party software applications or software application stores from prompting end users to decide [...on] their default."

7 Stuart Mills, Richard Whittle, Rafi Ahmed, Tom Walsh, Martin Wessel, *Dark patterns and sludge audits: an integrated approach*, Behavioural Public Policy (2023), 1–27, Cambridge University Press.

Browser freedom

One of the DMA's key tools to enable fair competition among browser makers is the prohibition for gatekeepers in Article 5(7) to "require end users to use, or business users to use, to offer, or to interoperate with" a web browser engine. This provision obliges Apple to allow other browser vendors what is absolutely common sense on literally any other operating system, namely to offer users their own browsers—complete with their competing browser engine—on devices running Apple's iOS operating system.

In order to comply with this new obligation, Apple has announced to indeed allow vendors to submit new app versions for their browsers that include a free choice of browser engine. Yet, in an apparent attempt to make this change in technology difficult for competitors and users alike, the gatekeeper has confirmed that it will require browser vendors to make the post-DMA version of their browser featuring their own engine a new and separate app. That is not only technically unnecessary but also means end users will be unable to simply upgrade to the new post-DMA browser of their choice. Instead, browser makers will have to inform their users about the new browser app, convince them to export their personal data (browsing history, bookmarks, settings, etc.), install the new, post-DMA browser, and re-import their data into the new browser.

Given how easily most users stick to defaults and how little average users know about the vital importance of browser engine diversity for the internet and for browser competition, this is an incredibly and entirely unnecessary hurdle that undermines compliance via artificial technical barriers to effective choice. We therefore consider the requirement for making the new post-DMA browser a separate app in the gatekeeper App Store a **direct breach of Article 13(4) DMA** which stipulates that the gatekeeper shall "not engage in any behaviour that undermines effective compliance with the obligations of Articles 5, 6 and 7 regardless of whether that behaviour is of a contractual, commercial or technical nature, or of any other nature, or consists in the use of behavioural techniques or interface design."

What is more, by requiring browser vendors to create a new app instead of offering their improved browser as an upgrade to end users, this also might have a direct effect on those post-DMA browsers' download numbers and ranking in the gatekeeper App Store. Low download numbers, in particular, would then also put into question Apple's compliance with its obligation under **Article 6(3) DMA**, as Apple has proposed that if a developer has multiple browser apps (which would be the case here: first the legacy version based on the gatekeeper's browser engine, and the post-DMA version with its own engine), "only the most downloaded app will be eligible" for inclusion in the list of browser choice options.[8] The new, more competitive post-DMA browsers would therefore be automatically excluded from the DMA's browser choice screen and its chances of successfully competing with the gatekeeper would be seriously and artificially reduced.

Furthermore, the terms and conditions that Apple forces upon browser vendors wishing to compete with the gatekeeper are in many aspects unfair, unreasonable, and discriminatory. For example,

8 Apple, *About the browser choice screen in iOS 17*, available at https://developer.apple.com/support/browser-choice-screen, last consulted on 8 April 2024.

Apple's "New Browser Engine Contract"[9] states that if a competing browser vendor fails to abide by any of Apple's terms (some of which are pretty vague and possibly in contravention and/or violation of the DMA themselves), the gatekeeper can not only reject app updates but also permanently remove and ban their browser app on all Apple platforms (presumably including macOS). As Mozilla spokesperson Damiano DeMonte has put it: "Apple's proposals fail to give consumers viable choices by making it as painful as possible for others to provide competitive alternatives to Safari."[10]

Interoperability

Apple introduced a request form for enabling interoperability with iOS on a case-by-case basis, which **violates Article 6(7) DMA**. This provision mandates free and automatic interoperability without a request, unlike Article 7(1) DMA. Currently however, Apple controls how and when to grant interoperability to developers without clear decision-making and timeframes.

Serious delays have impacted Free Software projects' competitiveness on iOS,[11] and arbitrary decisions could lead to discriminatory practices and self-preferencing. Without external audits or an appeal process, Apple's procedure is burdensome and deliberately complicates access to interoperability.

What is more, Article 6(7) prescribes an obligation for gatekeepers to enable interoperability between their devices and operating systems from third party manufacturers. Concretely, it obliges the gatekeeper to allow providers of services (here: operating system providers) effective interoperability with, and access for the purposes of interoperability to, the same hardware and software features accessed or controlled via the operating system (here: the firmware and hardware features the operating system interoperates with).

Furthermore, the same provision prescribes that the gatekeeper shall allow business users and alternative providers of services (here: operating systems providers) effective interoperability with, and access for the purposes of interoperability to, the same operating system, hardware or software features (here: the firmware and hardware features the operating system interoperates with) as are available to, or used by, that gatekeeper when providing such services.

Apple's Non-Confidential Summary of DMA Compliance Report is completely mute on this point[12] and so far, the gatekeeper's products 'iPhone' and 'iPad' do not allow interoperability with

9 Apple, *Web Browser Engine Entitlement Addendum for Apps in the EU*, available at https://developer.apple.com/contact/request/download/web_browser_engine.pdf, last accessed on 30 May 2024.

10 Emma Roth, *Mozilla says Apple's new browser rules are 'as painful as possible' for Firefox*, The Verge, 26 January 2024, available at https://www.theverge.com/2024/1/26/24052067/mozilla-apple-ios-browser-rules-firefox, last accessed on 30 May 2024.

11 "App review processes are opaque, and rules appear to be inconsistently applied, and could be used to favour Apple's and Google's own apps. Also, the resulting delays and uncertainty can add to development costs and hinder innovation by app developers.", Competition and Markets Authority (CMA), *Interim report (2022), Key findings*, available at https://www.gov.uk/government/publications/mobile-ecosystems-market-study-interim-report/interim-report, last accessed on 24 June 2024.

12 Apple, *Apple's Non-Confidential Summary of DMA Compliance Report*, 7 March 2024.

operating systems from third party manufacturers. Apple is therefore **not compliant with Article 6(7) DMA** to the detriment of competing mobile operating system providers.

Gatekeepers differ widely in how they currently enable operating system choice for users on devices sold by them. For example, x86-compatible hardware[13] for desktop and laptop PCs has a high level of standardisation, and devices using it enable the installation of a wide variety of operating systems, including Microsoft Windows, dozens of Linux variants, OpenBSD, FreeBSD and many others.

On Apple devices like iPhones and iPads, the situation is quite different: Both Apple devices and devices built for Google's Android operating system use ARM-based hardware instead of x86. As a hardware design feature, ARM enables the standardisation of devices' Base System Architecture (BSA) and Base Boot Requirements (BBR) through its 'SystemReady Program'. SystemReady was built to enable manufacturers and end users to securely and freely choose their operating system in a similar way as x86-compatible hardware already does.[14]

Yet, both Apple and Google have opted to not apply SystemReady, a decision that keeps users locked into the gatekeepers' own operating systems and prevents competing operating system vendors to enter the market for mobile devices and compete with the gatekeepers. Apple is therefore **not compliant with Article 6(7) DMA** to the detriment of competing mobile operating system providers.

***

13 x86 is a family of complex instruction set architectures for computer processors initially developed by Intel. Today, most desktop and laptop computers sold are based on the x86 architecture family, while mobile categories such as smartphones or tablets are dominated by ARM.

14 "Off-the-shelf OS interoperability across Arm-based platforms enables rapid, streamlined, and modern software deployment models for scale between market segments." ARM, *System Ready Key Benefits*, available at https://www.arm.com/architecture/system-architectures/systemready-certification-program, last accessed 24 June 2024.

Contacts

For further information and questions, please do not hesitate to reach out to any of the co-signatories:

ARTICLE 19
Mark Dempsey, Senior Advocacy Officer
markdempsey@article19.org

Cryptee
John Ozbay, Founder & CEO
info@crypt.ee

European Digital Rights (EDRi)
Jan Penfrat, Senior Policy Advisor
jan.penfrat@edri.org

F-droid App Store
Hans-Christoph Steiner, Technical Lead
team@f-droid.org

Free Software Foundation Europe (FSFE)
Lucas Lasota, Senior Project Manager
lucas.lasota@fsfe.org

Gesellschaft für Freiheitsrechte (GFF)
Svea Windwehr, Project coordinator
svea.windwehr@freiheitsrechte.org

Guardian Project
Nathan Freitas, Founder
nathan@guardianproject.info

Murena SAS
Rik Viergever, Public Affairs, Partnerships and Fair Tech
rik.viergever.ext@murena.com

Privacy International
Eliot Bendinelli, Programme Director
eliotb@privacyinternational.org

The App Fair Project
Marc Prud'hommeaux, Founder
marc@appfair.org