

22 October 2025

**APPLE'S BUSINESS TERMS RESTRICT THE ABILITY OF BUSINESS AND END USERS
TO INSTALL SOFTWARE AND SWITCH AND SUBSCRIBE TO DIFFERENT SOFTWARE
APPLICATIONS**

ARTICLE 19

&

GESELLSCHAFT FÜR FREIHEITSRECHTE

COMPLAINT

&

**REQUEST THAT THE EUROPEAN COMMISSION ADOPTS A NON-COMPLIANCE
DECISION**

Table of Contents

I. EXECUTIVE SUMMARY	3
II. INTRODUCTION	3
III. LEGAL FRAMEWORK.....	5
Article 6(4).....	5
Article 6(7).....	6
Necessity and proportionality	6
IV. APPLE’S CONDUCT	8
(A) Apple Developer Program (“ADP”) and Apple’s Developer Program License Agreement (“DPLA”).....	8
Violation of Article 6(4)	9
Necessity	10
Proportionality	10
Violation of Article 6(7)	11
Necessity	11
Proportionality	11
(B) Apple’s approach to software installation – Notarization	12
Violation of Article 6(4)	13
Necessity	13
Proportionality	14
Violation of Article 6(7)	15
Necessity	15
Proportionality	15
V. ACTION REQUESTED	15

I. EXECUTIVE SUMMARY

1. The Complaint provides evidence of Apple's conduct through its business terms and conditions governing its App Store, iOS and iPadOS operating system, which has caused, and continues to cause both a lack of interoperability with Apple devices and restrictions on installation and use of third-party software apps and app stores, which leads to harm to business users ("**developers**") and end users, in contravention with its obligations under the Digital Markets Act 2022 ("**DMA**").
2. By exercising control over the distribution of apps and app stores on its iPhone and iPad devices (hereafter "**devices**"), Apple engages in the below conduct, that is neither strictly necessary nor proportionate:
 - (a) Does not allow or technically enable the installation and effective use of third-party software apps or app stores using, or interoperating with, Apple's iOS and iPadOS (Article 6(4), DMA).
 - (b) Prevents third-party software applications or software application stores from prompting end users to decide whether they want to set that downloaded software application or software application store as their default (Article 6(4), DMA).
 - (c) Does not technically enable end users who decide to set that downloaded software application or software application store as their default to carry out that change easily (Article 6(4), DMA).
 - (d) Does not allow third-party apps or app stores, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same hardware and software features accessed or controlled via Apple's iOS and iPadOS (Article 6(7), DMA).
3. This Complaint supports the Commission's current investigation into Apple's business terms (Case DMA.100206) and urges the Commission to adopt a non-compliance decision pursuant to Article 29, DMA with respect to Apple's breach of Articles 6(4) and 6(7), DMA and impose a fine pursuant to Article 30, DMA. In addition, we ask that the Commission also (a) investigates Apple's "Notarization" system for third-party apps, which was expressly left open as a potential further investigation (see recital 23 of the Current Investigation (as such term defined below)¹), and (b) starts a specification procedure for any further specific measures that Apple should adopt to effectively disintermediate Apple's entrenched power over software distribution in iOS and iPadOS devices.

II. INTRODUCTION

4. This Complaint is made on behalf of the Gesellschaft für Freiheitsrechte e.V., a non-profit-organisation (registered under VR 34505 B at Amtsgericht Berlin-Charlottenburg), founded in 2015 that aims to protect and strengthen human and fundamental rights via litigation and other forms of legal intervention²; and ARTICLE 19 (company number: 02097222 registered in England and Wales), a charity founded in 1987 and based in the United Kingdom that propels the freedom of expression movement locally and globally through research, and legal and policy analysis.
5. We are writing further to the European Commission's investigation into Apple's business terms, and Apple's repeated attempts to ensure compliance with its obligations under the DMA. On

¹ https://ec.europa.eu/competition/digital_markets_act/cases/202431/DMA_100206_50.pdf

² Who we are - GFF – Gesellschaft für Freiheitsrechte e.V.

24 June 2024, the Commission published its decision to open proceedings with a view to the possible adoption of decisions (pursuant to Article 20(1), DMA) (the “**Current Investigation**”). The Commission is investigating Apple’s compliance with the obligations laid down in Articles 5(4), 5(7), 6(4), and 6(7), DMA.³ No decision of non-compliance has been made by the Commission, and we understand that as at the date of this Complaint, the investigation is still ongoing.

6. Apple’s business terms impose conditions on developers, which have the effect of preventing interoperability with third-party apps and app stores, and restricting end users’ accessibility to content since it reduces end user choice. Apple does not subject its own apps to the same rules thereby giving itself an unfair advantage⁴ and increasing lock-in effects, which stifles innovation within the app store and application markets and ultimately undermines market contestability. This leads to further power imbalance and a lack of inter-platform competition.
7. On 7 March 2024, Apple submitted to the Commission its compliance report. The Current Investigation is thus drafted further to the 2024 compliance report. On 7 March 2025, Apple published a further non-confidential summary of its compliance with the DMA (“**Apple’s 7 March 2025 Compliance Summary**”).⁵ However, the summary does not explain or justify the business term conditions nor their necessity or proportionality. Therefore, Apple’s conduct creates unnecessary barriers that limit access to the relevant functionality needed to operate on Apple devices.
8. We welcome the Commission’s previous and continuing work in upholding the provisions of the DMA. The Commission has already imposed fines on Apple regarding the anti-steering provisions for music streaming providers (DMA.100109⁶) and has closed consultations regarding proposed measures requesting interoperability within Apple’s systems (DMA.100204⁷ and DMA.100203⁸) due to Apple agreeing to modify its behaviour. However, Apple’s business terms are still the subject of a pending Current Investigation. This Complaint supports the Commission’s Current Investigation and avers that Apple’s practices amount to a breach of Articles 6(4) and 6(7), DMA.
9. The Current Investigation contains certain findings of fact that can also be supported by U.S. enforcement (albeit under a different law in a different jurisdiction and subject to different legal standards) following the U.S. Department of Justice’s (“**DOJ**”) antitrust lawsuit against Apple filed on 21 March 2024.⁹ The DOJ alleges that Apple illegally maintains a monopoly over smartphones by selectively imposing contractual restrictions on, restricting interoperability and withholding critical access points from app developers. The DOJ claims that Apple “strategically broadened, and aggressively enforced its App Store Guidelines to effectively block apps from hosting mini programs”¹⁰ and is seeking legal enforcement under the Sherman Act.

³ [DMA_100206_50.pdf](#)

⁴ See Recital 33 DMA, which states that an imbalance of rights can stem from where the gatekeeper offers a particular service that may also compete with business users.

⁵ <https://www.apple.com/legal/dma/NCS-March-2025.pdf>

⁶ https://ec.europa.eu/competition/digital_markets_act/cases/202523/DMA_100109_929.pdf

⁷ <https://digital-markets-act-cases.ec.europa.eu/cases/DMA.100204>

⁸ <https://digital-markets-act-cases.ec.europa.eu/cases/DMA.100203>

⁹ <https://www.justice.gov/atr/media/1344606/dl>

¹⁰ <https://www.justice.gov/atr/media/1344606/dl>, see para 67.

III. LEGAL FRAMEWORK

10. The DMA has regard to the Treaty of the Functioning of the European Union (“TFEU”) and refers to Articles 101 and 102 thereof but admits that the scope of these provisions were too limited to ensure the proper functioning of the internal market.¹¹ The DMA is thus designed to promote fairness and market contestability as an ex ante normative regulation aimed at guiding and shaping the behaviour of gatekeepers by setting out specific obligations on gatekeepers. Since they pursue similar objectives, the DMA aims to complement the enforcement of competition law without prejudice to Articles 101 and 102 TFEU.¹²
11. As a general principle, all firms, including dominant firms, have a freedom of contract and to choose their trading partners. However, Article 102 states that when a firm is dominant, it is restricted from carrying out certain conduct, which act in an abusive matter and in limited circumstances, be required to deal with certain third parties even if the platform is not indispensable for the commercial operation of the third-party.¹³
12. In addition to the obligations imposed by Article 102 TFEU, the DMA designates gatekeepers that have a combination of features that lead to serious imbalances in bargaining power and as a result, unfair practices and conditions for business users as well as for end users of core platform services provided by gatekeepers.¹⁴ They act as gateways for a large number of businesses.¹⁵ Apple has been designated as a gatekeeper and its operating system (iOS), app store (App Store) and web browser (Safari) as core platform services that are subject to the regulation.¹⁶
13. The DMA recognises that when vertically integrated, gatekeepers often have a dual role resulting in conflicts of interest because as an undertaking providing a software application store to business users as well as software applications, they reserve themselves a better position by (a) restricting third-party alternative app store businesses from operating in their operating system, and (b) not imposing such conditions and terms onto their own app store and/or applications. Apple is one of such businesses that has such conflicts of interest (Recital 51, DMA).
14. Of particular relevance for this Complaint, the DMA is aimed to help third-party apps and app stores emerge and function as genuine competitors to the gatekeeper by limiting unfairness in markets where the gatekeeper obtains a disproportionate advantage and raises significant barriers to entry. In practice, however, Apple’s business terms prevent such competition from developing, thereby frustrating the broader objectives of the DMA.

Article 6(4)

15. Article 6(4) DMA states that a gatekeeper shall “allow and technically enable the *installation and effective use of third-party software applications or software application stores* using, or

¹¹ Recitals 2 to 4, DMA

¹² Recital 10 to 11, DMA

¹³ See [case C-233/23: Alphabet and Others](#), which states that the “platform is interoperable with an app developed by that third-party undertaking is capable of constituting an abuse of a dominant position even though that platform is not indispensable for the commercial operation of that app on a downstream market, but is such as to make that app more attractive to consumers, where that platform has not been developed by the undertaking in a dominant position solely for the needs of its own business”

¹⁴ Recitals 2 to 4, DMA

¹⁵ Recital 6, DMA

¹⁶ Decision C(2023) 6100

interoperating with, its operating system”. The aim of Article 6(4) DMA is universal compatibility of all apps and app stores with a gatekeeper’s operating system. The requirement of allowing and enabling effective use must be interpreted in light of the aim of Article 6(4) DMA to remove restrictions on distribution through the rules established by a gatekeeper.

Article 6(7)

16. Article 6(7) DMA states that a gatekeeper shall “allow providers of services and providers of hardware, *free of charge, effective interoperability* with, and access for the purposes of interoperability to, the same hardware and software features accessed or controlled via the operating system”. Interoperability is defined in Article 2(29) DMA as the “ability to exchange information and mutually use the information which has been exchanged through interfaces or other solutions, so that all elements of hardware or software work with other hardware and software and with users in all the ways in which they are intended to function”.
17. The purpose of the interoperability obligation in Article 6(7) DMA is to create a ‘level playing field’ in markets for services or hardware where the gatekeeper may have an advantage due to its control over the operating system. Interoperability is critical as it enables providers of products and services to effectively create new value – it addresses the competitive advantage that a gatekeeper enjoys due to its dual role.
18. Interoperability is essential to safeguarding user choice and supplier access to consumers, which is why the DMA recognises the significant influence gatekeepers can wield in undermining interoperability and suppressing competitive dynamics within a market – raising contestability and fairness concerns. Gatekeepers have a responsibility to ensure operability due to their position, and the DMA explicitly requires that such interoperability be provided free of charge.
19. Furthermore, the interoperability has to be “effective”, applied in a non-discriminatory fashion on equal conditions (see recital 57, DMA), free of any undue restrictions. The gatekeeper must not impose unnecessary technical requirements or require unnecessary certifications that limit access to the relevant functionality. The Commission explains that “effective interoperability depends on the gatekeeper’s choices regarding the design of its operating system. For some features a mere lifting of a contractual or technical restriction might be sufficient. In other cases, the gatekeeper might need to implement the prerequisites – including software components – that are required to provide effective interoperability.”¹⁷

Necessity and proportionality

20. Both Article 6(4) and Article 6(7) of the DMA provide that a gatekeeper shall not be prevented from taking measures that would otherwise limit the obligations set out in those provisions, *to the extent that such measures are strictly necessary and proportionate*. Recital 50 of the DMA states that these measures can be “technical or contractual”, which can include (a) design options to protect the hardware or operating system against unauthorised access, (b) settings enabling end users to effectively protect security in relation to third-party software applications or software application stores. In the case of both Articles, it is for the gatekeeper, knowing its

¹⁷ See [CASE DMA.100204](#), recital 74

products or services best, to decide what measures are necessary and provide a justification of their necessity and proportionality.¹⁸

21. To be “strictly necessary” means that there are no less restrictive means¹⁹ available to Apple to achieve the same purpose it sets out to, whereas proportionality implies that Apple’s measures must be put in relation to resulting restrictions on third-parties. In the 23 April 2025 non-compliance decision against Apple for DMA infringements as a result of its anti-steering provisions,²⁰ the Commission analysed whether Apple had shown that there are “no less far-reaching measures that could achieve the same objectives”.²¹ The Commission also analysed Apple’s actions and the impact on app developers’ incentives to use alternative distribution channels, which can reinforce Apple’s App Store and reduce contestability in app stores.²²
22. In terms of proportionality, the Commission ultimately found that Apple’s 10% - 17% commission fee on end users’ purchases (either within the app installed on the App Store or outside the app for transactions completed by end users within 7 calendar days after link-out from the developer’s app, of digital goods and services from app developers) was not proportionate for the implementation and development of the steering service that Apple provides. It did not consider that the fee was remuneration for facilitating the initial acquisition of the end user by the app developers.²³
23. Pursuant to Article 6(4) DMA, this exception applies where the gatekeeper seeks to ensure that third-party software applications or software application stores do not endanger the *integrity of the hardware or operating system*, or to apply settings enabling end users to protect security effectively.
24. Pursuant to Article 6(7) DMA, this exception applies to measures necessary to ensure that interoperability *does not compromise the integrity* of the operating system, virtual assistant, hardware, or software features provided by the gatekeeper.
25. Any justification of necessary and proportionate measures should be in relation to the integrity of the operating system, which refers specifically to the state of being unimpaired (i.e., the correct and reliable functioning of the operating system or hardware features, free from unauthorised manipulation or corruption).²⁴ In defining this term, the Commission explicitly draws on the Cyber Resilience Act (“CRA”), which links integrity to the absence of manipulation or modification “not authorised by the user”.²⁵ The Commission’s interpretation under the DMA aligns integrity with the CRA’s technical notion of protection against unauthorised interference, while rejecting the broader, more subjective justifications based on privacy, safety, or “trust.” Integrity, in this sense, protects the system, not the business model of Apple.²⁶ Apple may invoke integrity only when they can demonstrate, with verifiable evidence, that interoperability and third-party software would concretely impair the functioning

¹⁸ Recital 50, DMA with regard to the requirement in Art. 6(4)(2): “if the gatekeeper demonstrates”.

¹⁹ Recital 50, DMA.

²⁰ https://ec.europa.eu/competition/digital_markets_act/cases/202523/DMA_100109_929.pdf

²¹ https://ec.europa.eu/competition/digital_markets_act/cases/202523/DMA_100109_929.pdf, recital 116.

²² https://ec.europa.eu/competition/digital_markets_act/cases/202523/DMA_100109_929.pdf, recital 160.

²³ https://ec.europa.eu/competition/digital_markets_act/cases/202523/DMA_100109_929.pdf, recitals 180 to 198.

²⁴ Recital 50, DMA, states that the operating system should be “protected against unauthorised access, by ensuring that security controls specified for the hardware or the operating system concerned cannot be compromised”.

²⁵ See Paragraph 83 of DMA.100204 – Apple – Operating Systems – iOS – Article 6(7) – SP – Process. Decision of 19 March 2025 – Final Measures. https://ec.europa.eu/competition/digital_markets_act/cases/202523/DMA_100204_2073.pdf.

²⁶ See Paragraph 87 of DMA.100204 – Apple – Operating Systems – iOS – Article 6(7) – SP – Process. Decision of 19 March 2025 – Final Measures. https://ec.europa.eu/competition/digital_markets_act/cases/202523/DMA_100204_2073.pdf.

of the operating system or its security control - and any such measures must be strictly necessary, proportionate, non-discriminatory, and independently verifiable. The prerogative to install software lies with the user, not with the gatekeeper.²⁷

IV. APPLE'S CONDUCT

(A) Apple Developer Program ("ADP") and Apple's Developer Program License Agreement ("DPLA")

26. To develop apps for distribution in Apple's App Store, a developer must join the Apple Developer Program ("ADP").²⁸ For the use of, *inter se*, the possibility to, free of charge, communicate and promote offers to end users acquired via the App Store or through other channels, and to conclude contracts with those end users, a business user must agree to and not be in violation of the latest version of Apple's Developer Program License Agreement ("DPLA")²⁹, which requires, *inter alia*, enrolment in the Apple Developer Agreement and to sign up to the Alternative Terms Addendum for Apps in the EU.³⁰
27. As per the Alternative Terms Addendum for Apps in the EU, Apple has conditioned the provision of a third-party app store as a native app in its iOS and iPadOS subject to the requirement of the Alternative App Marketplace Entitlement. This is only granted if certain requirements are fulfilled by the provider of the third-party app store: either (1) provide and maintain a stand-by letter of credit in the amount of €1,000,000 from a financial institution that is at least A-rated; or (2) be a member of good standing in the Apple Developer Program for two continuous years or more and have an app that had more than one million first annual installs on iOS and iPadOS in the EU in the prior calendar year.
28. When these conditions are put into context, Standby Letters of Credit ("SBLCs")³¹ are used in other industries where payment risks, and hence non-payment risks arise, as a guarantee of payment to a seller and banks typically charge issues fees for SBLCs that commonly range between 0.25% to 2% annually (and in some cases up to 10% depending on risk).³² This fee is effectively meant to scale with the bank's maximum exposure, aligning with duration and covering any associated costs so the percentage charged is thus dependent on risk. This would mean that a €1,000,000 SBLC can impose a recurring annual cost and collateral requirements that many SMEs cannot meet.
29. The effects of Apple's behaviour are already visible. The "App Fair Project", a non-profit charitable organization that was founded as a worldwide nexus for free apps to be built, distributed and maintained, is publicly appealing for support either to raise the substantial sum of €1,000,000 or else surpass one million downloads of an app through Apple's App Store.³³ The App Fair Project have stated that the alternative app marketplace that Apple has is "insufficient for the needs of a truly independent app distribution system".³⁴

²⁷ See Paragraphs 84, 104 and 107 of DMA.100204 – Apple – Operating Systems – iOS – Article 6(7) – SP – Process. Decision of 19 March 2025 – Final Measures. https://ec.europa.eu/competition/digital_markets_act/cases/202523/DMA_100204_2073.pdf.

²⁸ [Choosing a Membership - Support - Apple Developer](#)

²⁹ <https://developer.apple.com/support/terms/apple-developer-program-license-agreement/>

³⁰ https://developer.apple.com/contact/request/download/alternate_eu_terms_addendum.pdf

³¹ <https://www.tradefinanceglobal.com/letters-of-credit/standby-letter-of-credit-sblc/>

³² <https://www.fgcapitaladvisors.com/standby-letters-of-credit-what-they-cost-and-how-sponsors-can-raise-the-margin>

³³ [The App Fair Project | The universal free and open-source app marketplace](#)

³⁴ [App Fair Retrospective, 2024 | The App Fair Project](#)

Violation of Article 6(4)

30. Apple's business terms (Apple's Alternative Terms Addendum for Apps in the EU) go in contravention to this obligation in the market for "software application stores" for the following reasons:
- (a) The App Store functions as an intermediary platform for the distribution of applications, over which Apple exercises complete control through stringent requirements. A €1,000,000 stand-by letter of credit functions as a de facto tax on competing app stores, operating as a barrier to entry and expansion, effectively excluding small and medium-sized developers, new entrants, and expanding smaller businesses who are unlikely to have the financial capacity to secure such credit. For them, the only alternative is to demonstrate continuous membership in the Apple Developer Program for at least two years *and* to operate an app that has achieved more than one million first annual installs on iOS and iPadOS in the EU. These are arbitrary restrictions that limit third-parties' app stores' ability to effectively use Apple's operating system to reach its end users.
 - (b) As the evidence of this Complaint demonstrates, Apple's requirements lack any reasonable calibration. These requirements apply regardless of app type, business model, proven harm or previous credit history and non-payment risk. Apple ignores the availability of less restrictive alternatives (i.e. insurance and escrow frameworks). Such overarching requirements are against the expected diligence of a dominant infrastructural platform (as per its obligations under competition law as well as the DMA, which are summarised in paragraphs 10 to 25 above) and do not align with the expectations of the software industry.
 - (c) The result of such conduct is the limitation on and exclusion of small developers, new entrants, and expanding businesses, thereby restricting those who may operate within its app store. Through restricting third-party software installation, this provides Apple with an unfair advantage. The limitation entrenches Apple's own app store and prevents contestability in the alternative app and app store markets. This DMA obligation emphasises that the installation right of third party-software applications should be "effective". The DMA explains that any restrictions that can "limit the ability of developers of software applications to use alternative distribution channels and the ability of end users to choose between different software applications from different distribution channels" undermines the ability of end users to effectively use third-party software applications or app stores.³⁵ The Commission's investigation centres around whether Apple's business terms allow for alternative channels of distribution or whether there are any terms that unduly restrict this.³⁶ The restrictions that Apple imposes contravene the "effective" use of third-party apps and app stores obligations as set out in Article 6(4) DMA.
 - (d) Apple's refusal to permit third-party software installation, specifically apps and app stores, except in highly limited circumstances, as outlined in its Web Distribution policy, allows Apple to maintain strict control over the app distribution channel of its devices. This not only undermines developers' ability to compete effectively with Apple's App Store, impacting contestability, but also constrains end user choice by limiting access to only those apps that

³⁵ Recital 50, DMA

³⁶ Recital 17, [Current Investigation](#)

Apple deems admissible. Furthermore, these restrictions hinder technological innovation,³⁷ as third-parties are forced to operate within the confines of Apple’s guidelines, suppressing potentially novel approaches to app development and distribution. End users are consequently confined within Apple’s “walled garden” ecosystem.

31. In June 2025³⁸, Apple announced an update to its policy to demonstrate compliance with the DMA. However, this update applies solely to the communication and promotion of offers and does not address the fundamental restrictions on third-party app stores or interoperability. As such, it fails to remedy Apple’s non-compliance with Articles 6(4) and 6(7), DMA.

Necessity

32. Apple’s Alternative Marketplace entitlement conditions of either a €1,000,000 stand-by letter of credit or being a “member of good standing” (see further in paragraph 27 above) go beyond the limits of what is necessary regarding ensuring the integrity of the operating system. Apple ignores less restrictive alternatives (i.e. insurance and escrow frameworks), and provides no justification for doing so.

Proportionality

33. As outlined in paragraph 30(a) – (d) above, the annual cost of paying for such a letter of credit imposes a burden on SMEs that is expensive and impacts their business model and costs. Such costs risk being passed on to further apps and/or end users. For example, an alternative app store “AltStore” used to charge its hosted apps €1.50 (plus tax) as a result of Apple’s costs (the Core Technology Fee) until AltStore received a grant from *Fortnite*.³⁹
34. The decision to require a €1,000,000 stand-by letter of credit appears to be set at an arbitrary level. This amount is inevitably likely to exclude smaller businesses that have a short trading history, but which may be running very successful and growing internet businesses. For example, a business that has started up and generated significant volumes of users will be well on its way to develop traction with those users and as is typical for internet businesses, they often start charging users later down the line when the product is understood and appreciated by customers. WhatsApp started in this way: WhatsApp had reached approximately 700 million users by April 2015. It only later implemented a subscription model, charging a small annual fee after the first year to maintain a user base that was not interested in advertising. The fee was never paid because the business was sold to Facebook for \$19bn.⁴⁰ The practice of generating significant scale before generating revenue is known as “Blitzscaling”⁴¹ which is a chaotic process, and such businesses are often very limited in their access to cash and funds. Investors and financiers may have significant difficulty in providing or supporting a €1,000,000 stand-by letter of credit.
35. The requirement to be a “member of good standing” in the Apple Developer Program for a minimum of two continuous years in addition to having an app with more than one million first annual installs on iOS and iPad OS in the prior year is also an arbitrary limit. Since technology

³⁷ As Abigail Slater emphasised in her speech on 16 September 2025: “Entrepreneurs and innovators will reshape our world for the better if they have that freedom, but if they are blocked by exclusionary practices and regulations, we won’t ever know what could have been.” (Accessible at <https://www.justice.gov/opa/speech/assistant-attorney-general-gail-slater-delivers-keynote-address-2025-georgetown-law>)

³⁸ <https://developer.apple.com/news/?id=awedznci>

³⁹ <https://www.theverge.com/2024/8/14/24220623/altstore-pal-third-party-app-store-drops-subscription-epic-grant>

⁴⁰ <https://en.wikipedia.org/wiki/WhatsApp>

⁴¹ <https://hbr.org/2016/04/blitzscaling>

businesses need visibility with which to grow their user base, they need distribution. Apple is one of the main distribution systems for apps to reach consumers and its products provide the opportunity for apps to be seen by the members of Apple's over 1.4 billion user base. Having to have more than one million first annual installs is a high threshold for a small and expanding business; Apple's restrictions will act as a barrier to entry and expansion, and if set at all should be at a much lower threshold.

Violation of Article 6(7)

36. Apple's conduct has, and continues to, deprive third-party developers in contravention of the obligation in Article 6(7) DMA in the following ways:
- (a) Apple only allows access to alternative software distribution channels through its Alternative Terms Addendum for Apps in the EU, which contain conditions that are stringent, arbitrary and exclusionary; and
 - (b) Apple has chosen to require a request form to enable interoperability with iOS and iPhone features on a case-by-case basis.⁴² This approach is inherently uncertain and lacks transparency, leaving full discretion firmly in Apple's remit. By conditioning interoperability in this way, Apple fails to comply with Article 6(7) DMA, which obliges gatekeepers to ensure interoperability with their hardware and software features in a manner that is effective and free of undue restrictions.
37. In June 2025⁴³, Apple announced an update to its policy to demonstrate compliance with the DMA. However, this update applies solely to the communication and promotion of offers and does not address the fundamental restrictions on third-party app stores or interoperability. As such, it fails to remedy Apple's non-compliance with Article 6(7) DMA.

Necessity

38. Apple's Alternative Marketplace entitlement conditions (as outlined in paragraph 27 above) ignore less restrictive alternatives (i.e. insurance and escrow frameworks). Apple provides no justification for the high barrier to entry that the stand-by letter of credit brings to SMEs and new entrants.

Proportionality

39. Apple adopting a process of requesting a 1 million stand-by letter of credit rather than a percentage disproportionately affects SMEs. This discriminates by size which, unlike adopting a percentage approach, is inaccessible for SMEs, startups and new entrants.
40. In Apple's 7 March 2025 non-confidential summary of its compliance with the DMA obligations, Apple introduces measures to allow alternative app marketplaces to operate as native apps and to also allow Web Distribution. To "mitigate, insofar as possible, the risks introduced by the allowance of alternative app marketplaces and Web Distribution", Apple states that they have adopted a "baseline level of review" of, and "minimum standards for alternative app marketplaces (Alternative App Marketplace Entitlement)". No further detail regarding the justification of why these measures are needed for preserving the integrity of the operating system is provided by Apple.

⁴² <https://developer.apple.com/support/ios-interoperability/>

⁴³ <https://developer.apple.com/news/?id=awedzncl>

(B) Apple's approach to software installation – Notarization

41. The technical architecture of the web enables “any-to-any” interoperability. “Sideloading” refers to the practice of installing software on a device that enables access to the worldwide web without using the gatekeeper’s app store or software distribution channel.⁴⁴ Apple permits sideloading only in very limited circumstances, rendering the practice effectively inoperable.
42. Apple’s Web distribution allows authorised developers to distribute their iOS and iPadOS apps to users in the EU directly from a website owned by the developer. However, apps offered through Web Distribution must meet Apple’s Notarization requirements⁴⁵ with Apple’s proprietary encryption and can only be installed from a website domain that the developer has registered in App Store Connect.⁴⁶ Apple has diverse Notarization procedures among its operating systems. Curation is handled differently for Apple’s Mac devices in comparison with iPhones and iPads. Apple does not impose stringent Notarization rules on Mac desktops and laptops. In MacOS, developers and end users have access to unfettered third-party software installation without the DRM-based encryption system for distribution. Apple’s *Enterprise Distribution Program*⁴⁷ allows organisations to create, sign, and distribute apps directly to users without intervention by Apple. Through this program, Apple effectively permits sideloading on iOS and iPadOS devices, but allows this only for large companies. Lastly, Apple also allows sideloading of Apple Music (in the form of the applemusic.apk file) on Android devices but does not permit similar direct sideloading of, for instance, the Spotify.ipa file on iOS.⁴⁸ These examples above demonstrate that Apple already has the infrastructure and security protocols in place to allow third-party app distribution outside the App Store.
43. Apple creates obscurity over source code. When Apple’s App Review is applied to sideloading and enabling competing app stores, App Review means a subsequent re-signed and encrypted binary with proprietary DRM, which iOS and iPadOS require in order for software to be installed. Then, the app’s binary code is provided in an encrypted manner via the App Store to the public. The introduction of an opaque layer of encryption over source code blocks the inspection of the source code by third-party auditors and does not allow a credible reproducible build of the app. Forcing such proprietary encryption via DRM over the submitted code has serious implications towards security – as third-party auditors cannot certify the authenticity of the source code. It is not possible to further audit the app’s source code, since a credible reproducible build of the app is no longer possible without breaking Apple’s DRM.
44. As of the time of writing, Apple’s website outlines only the procedure for submitting applications for Notarization, without providing any detail as to the substantive criteria or process involved. This lack of transparency deprives developers of meaningful insight into the decision-making framework, leaving Apple with unilateral control over what appears to be arbitrary decision making since no justification for the Notarization procedure was provided by Apple in Apple’s 7 March 2025 Compliance Summary. In addition, the requirement that a

⁴⁴ <https://www.howtogeek.com/773639/what-is-sideload-and-should-you-do-it/>

⁴⁵ <https://developer.apple.com/help/app-store-connect/managing-alternative-distribution/submit-for-notarization>

⁴⁶ <https://developer.apple.com/support/web-distribution-eu/>

⁴⁷ See the instructions webpage for the Apple Developer Enterprise Program, available at: <https://developer.apple.com/programs/enterprise/>.

⁴⁸ See Apple’s documentation for Android: “Looking for Apple Music for your Android phone?”: <https://web.archive.org/web/20250412175450/https://www.apple.com/lae/apple-music/android-download/>

developer's website domain be registered through App Store Connect further entrenches dependence on Apple's ecosystem, reinforcing its gatekeeper position.

45. In order to access the App Store Connect, the App Store Connect API and the associated developer applications for iPhone and iPad devices, developers are required to maintain an active Apple Developer account. Obtaining such an account entails the payment of an annual fee of 99 USD and acceptance of the Apple Developer Program's terms and conditions. Holding an Apple Developer Account is the only way by which developers can apply for entitlements to enable competing app distribution, as well as for distribution through the Apple App Store. The transparency of a third-party app being accepted onto App Store Connect is limited and vague and opaque, which consolidates gatekeeping control over software distribution in iOS and iPadOS devices.⁴⁹ The imposition of requiring such an account preserves Apple's ability to have unilateral conduct. For example, Apple blocked Epic Games' developer account, which restricted Epic Games' ability to launch the Epic Games Store and removed its game Fortnite from iOS.⁵⁰
46. Further, to use App Store Connect, a third-party app store or app developer will need to enrol on the Apple Developer Program. Without a developer account, it is not possible to submit apps to the app stores. Therefore, the Notarization requirements are only further compounded as Apple notes that to utilise Web Distribution, a developer needs to agree to the Alternative Terms Addendum for Apps in the EU. Thus, a developer must meet the same pre-requisites as outlined in paragraph 27 above. This suffers from the issues set out in paragraph 30 of this Complaint, notably the restrictions on entry and expansion and exclusion of small developers and restricting user access to content.

Violation of Article 6(4)

47. Apple's Notarization procedure is in contravention to this obligation in the market for "software application stores". Third-party apps and app stores need to go through Apple's Notarization procedure without any guidance or details regarding the process to achieve such Notarization. This sets forth a condition for third-party apps to be distributed in iOS and iPadOS, which is restrictive in its application. This does not fulfil the "effective" use of third-party apps and app stores as set out in Article 6(4) DMA.
48. Similarly as for the ADP, in June 2025⁵¹, Apple's announced update to its policy to demonstrate compliance with the DMA applied solely to the communication and promotion of offers and does not address the fundamental restrictions on third-party app stores or interoperability. As such, it fails to remedy Apple's non-compliance with Article 6(4) DMA.

Necessity

49. Article 6(4) DMA does include a safe harbour where the gatekeeper is able to take measures that are "strictly necessary and proportionate" to "protect security in relation to third-party software applications or software application stores" provided that these measures are "duly justified" by the gatekeeper.

⁴⁹ [Become a member - Apple Developer Program](#)

⁵⁰ <https://www.epicgames.com/site/en-US/news/apple-terminated-epic-s-developer-account>

⁵¹ <https://developer.apple.com/news/?id=awedzncl>

50. The Notarization requirements, necessary to offer apps through Web Distribution, suffers from a lack of transparency that represents an overly restrictive means for Apple to supposedly protect the integrity of iOS and iPadOS. Furthermore, the third-party app can only be installed from a website domain that the developer has registered in App Store Connect and the third-party app must fulfil the same requirements as Apple's Alternative Marketplace Entitlement conditions. It thus suffers from the same violations as noted in paragraph 30. Apple describes the Notarization process as the "baseline level of review....focused on platform policies for security and privacy and to maintain device integrity".⁵² However, no further detail is provided regarding why the Notarization requirements are necessary for maintaining such integrity.
51. The need for an app to also fulfil the same conditions of the Alternative Terms Addendum for Apps in the EU with either a stand-by letter of credit or to be a member of good standing does not seem to be needed for any non-payment risk. Apple's fee structures demonstrates that for apps in Apple's App Store, whenever a payment is made between the app and the end user for digital goods, the billing goes through Apple. If a physical item is purchased through an app, the app can use whichever billing system it likes (e.g., a physical book sold in the Amazon app can use Amazon's own billing system). In contrast, for digital goods, billing needs to go through Apple, from which Apple extracts a commission (e.g., if an ebook is purchased from the Amazon Kindle app, the billing must use Apple's own in-app payment system, which they use to automatically deduct their fee). Therefore, any non-payment risk is already controlled via the Notarization procedure where an app needs to go through Apple's App Review. The additional conditions of the Alternative Terms Addendum for Apps in the EU are thus redundant and unnecessary for any issues of credit risk.
52. Further, Apple's claim that the Notarization procedure is necessary for security is negated by the fact that (a) such a Notarization procedure means that Apple has centralised control, which creates a single point of failure, and (b) the number of cybersecurity breaches that Apple suffers.⁵³
53. Instead, an alternative viable model could be that third-party developers should be able to distribute their apps without the need for Notarization. For that goal, third-party developers should be able to (a) generate their own signing certificates; (b) sign their own app binaries, being able to perform reproducible builds; and (c) have access to open and well-documented app installation APIs.

Proportionality

54. As noted above in paragraph 42, Apple has diverse Notarization procedures among its operating systems. Curation is handled differently for Apple's Mac devices in comparison with iPhones and iPads.⁵⁴ This demonstrates that Apple already has the infrastructure and security protocols in place to allow third-party app distribution outside the App Store so any justification of the Notarization procedure on grounds of proportionality also cannot stand. Apple sells Mac devices (laptops and desktops) under significantly less restrictive policies, where many companies compete to offer privacy and security to consumers and business users (e.g., anti-

⁵² <https://www.apple.com/legal/dma/NCS-March-2025.pdf>, page 15

⁵³ See, for example, the June 2025 cyber breach that exposed login credentials and passwords of Apple users at <https://www.independent.co.uk/tech/security/google-data-breach-facebook-apple-passwords-leaked-b2776613.html>

⁵⁴ See Apple's documentation for Android: "Looking for Apple Music for your Android phone?": <https://web.archive.org/web/20250412175450/https://www.apple.com/lae/apple-music/android-download/>

virus systems, etc.). In macOS, developers can sell their product directly to Mac users and users can directly install any software from any source. Despite this, Apple still assures consumers that Mac devices are secure. There is no reason why security around iPhones, iPads or other devices should be any different. Even theoretically, it is unclear why reliance on one company's decisions and solutions, instead of the market mechanism, should be a superior way to assure the best possible security and privacy of consumers.

Violation of Article 6(7)

55. As outlined above, the third-party app can only be installed from a website domain that the developer has registered in App Store Connect and the third-party app must fulfil the same requirements as Apple's Alternative Marketplace Entitlement conditions (thereby violating Article 6(7) in the same way as noted in paragraphs 36 to 37). The lack of transparency in the Notarization procedure does not fulfil the Commission's definition of what is "effective interoperability" since it presents contractual and technical restrictions on third-parties. These restrictions merely preserve Apple's unilateral control, and the significant influence Apple keeps over its iOS.

Necessity

56. As noted above in paragraph 40, in Apple's 7 March 2025 non-confidential summary of its compliance with the DMA obligations, Apple introduces measures to allow alternative app marketplaces to operate as native apps and to also allow Web Distribution. To "mitigate, insofar as possible, the risks introduced by the allowance of alternative app marketplaces and Web Distribution", Apple states that they have adopted a "baseline level of review" of apps (Notarization). No further detail regarding the justification of why these measures are needed for preserving the integrity of the operating system is provided by Apple.

Proportionality

57. As noted above in paragraph 42, Apple has diverse Notarization procedures among its operating systems. Curation is handled differently for Apple's Mac devices in comparison with iPhones and iPads. This demonstrates that Apple already has the infrastructure and security protocols in place to allow third-party app distribution outside the App Store. This suggests that the measures put in place by Apple are not necessary to protect the "integrity of the operating system" as such concerns would otherwise not have prevented Apple from taking a more lenient approach with its Mac devices.

V. ACTION REQUESTED

58. We note that the issues outlined in this Complaint are relevant for most, if not all, app developers and Apple users in the digital ecosystem. However, for the purposes of the Complaint and relevance to the current Commission investigation, we are focusing on issues that relate to Article 6(4) and Article 6(7), DMA. This is without prejudice to the broader objectives of the DMA in ensuring that gatekeepers do not distort competitive market dynamics and that innovation is able to flourish where the Commission is also able to open a dialogue with the gatekeeper to comply with the obligations under the DMA (see recital 65, DMA).
59. This Complaint reflects findings and observations that are intended to assist the Commission in its Current Investigation into Apple's business terms. This Complaint acts as a formal submission that Apple's business terms governing its App Store, iOS and iPad OS enable Apple

to restrict competition in the app distribution market by providing itself an unfair advantage, impacting contestability, and restricting end users' access to content by exerting disproportionate and unjustified control over the availability and operation of alternative third-party app stores and apps.

60. Further, Apple's actions provide evidence that the Commission should also open proceedings on the Notarization system implemented by Apple, which the Commission considered possible in June 2024⁵⁵ and which, as demonstrated herein, has become urgent.

61. Therefore, we urge the Commission to:

- (a) Adopt a non-compliance decision pursuant to Article 29 DMA with respect to Apple's breach of Articles 6(4) and 6(7) DMA and impose a fine pursuant to Article 30 DMA; and
- (b) Investigates Apple's "Notarization" system for third-party apps, which was expressly left open as a potential further investigation (see recital 23 of the Current Investigation);
- (c) Start a specification procedure to specify, with the support of industry players, including non-profit ones, and other relevant stakeholders, the measures that Apple should adopt to effectively disintermediate Apple's entrenched power over software distribution in iOS and iPadOS devices.

⁵⁵ Footnote 4, recital (23)