7 March 2024

Apple's Non-Confidential Summary of DMA Compliance Report

iOS, Safari, and the App Store are part of an integrated, end-to-end system that Apple has designed to help protect the safety, security, and privacy of our users, and provide a simple and intuitive user experience. We strive to earn users' trust by promptly resolving issues with apps, purchases, or web browsing through App Review, AppleCare customer support, and more.

The DMA requires changes to this system that bring greater risks to users and developers. This includes new avenues for malware, fraud and scams, illicit and harmful content, and other privacy and security threats. These changes also compromise Apple's ability to detect, prevent, and take action against malicious apps on iOS and to support users impacted by issues with apps downloaded outside of the App Store.

Apple is introducing protections — including Notarization for iOS apps, an authorization for marketplace developers, and disclosures on alternative payments — to reduce risks and deliver the best, most secure experience possible for users in the EU. Unfortunately, even with these measures in place, many risks remain. Apple will continue to seek to introduce new protections over time to address some of those risks. And Apple will continue to urge the European Commission to allow it to take other measures to protect its users.

The user safeguards and developer tools and technologies we've built reflect Apple's commitment to iPhone and iOS remaining the safest mobile platform users can choose in Europe, and the app ecosystem that offers all developers the greatest opportunity.

Developers can use these new options in Xcode 15.3 and iOS 17.4. The changes became available to users in the 27 EU member countries beginning in early March 2024.

Alternative distribution on iOS in the EU

Developers will be able to create alternative marketplace apps on iOS. In iOS 17.4, Apple provides authorized marketplace developers access to new app marketplace frameworks and APIs that let them receive and retrieve notarized apps[1] from Apple Developer Program members securely, let users download and install marketplace apps from their website with authorized browsers, integrate with system functionality, back up and restore users' apps, and more. Using new App Store Connect distribution tools, developers can choose

[1] See more about notarized apps below.

to notify users of any app updates, so users can be offered important functionality like automatic app updates.[2]

Alternative distribution poses increased privacy, safety, and security risks for users and developers. This includes risks from installing software that compromises system integrity with malware or other malicious code, the distribution of pirated software, exposure to illicit, objectionable, and harmful content due to lower content and moderation standards, and increased risks of scams, fraud, and abuse.

It's important to understand that some features may not work as expected for apps using alternative distribution. Features like Screen Time, parental controls, and Spotlight continue to function and maintain Apple's security, privacy, and safety standards. Features like restrictions on In-App Purchase in Screen Time and Family Purchase Sharing, universal purchase, as well as Ask to Buy are not supported on alternatively distributed apps because the App Store and its private and secure commerce system are not facilitating these purchases. Apple isn't able to assist users with refunds, purchase history, subscription cancellations and management, violations of user data privacy, abuse, or fraud and manipulation, in addition to issues that make the user experience less intuitive. Developers, or the alternative app marketplace from which their app was installed, are responsible for addressing such issues with customers.

The terms applicable to Developers wishing to create alternative app marketplaces or distribute apps through alternative app marketplaces are set forth in the Alternative EU Terms Addendum.[3]

Distributing on an alternative app marketplace

When considering distribution on an alternative app marketplace, developers should evaluate the marketplace's offering and terms and conditions — including any financial obligations, approval processes and policies, and legal protections — before setting up alternative distribution in App Store Connect. Marketplace apps may only be installed from the marketplace developer's website.

To authorize an app marketplace to distribute an app, a developer must contact the marketplace developer to receive a security token required for alternative distribution. The app developer can add and remove marketplaces and select which apps they intend to distribute on each marketplace in App Store Connect.[4]

---

2 For more details see https://developer.apple.com/support/alternative-app-marketplace-in-the-eu/ and https://developer.apple.com/documentation/marketplacekit.

3 For more details see https://developer.apple.com/support/dma-and-apps-in-the-eu/#distribution-eu.

4 For more details see https://developer.apple.com/help/app-store-connect/distributing-apps-in-the-european-union/manage-distribution-on-an-alternative-app-marketplace.

Using new App Store Connect distribution tools, developers are able to easily download their signed binary assets to transfer them directly to a marketplace for distribution. Developers can also take advantage of new support in the App Store Connect API to let a marketplace retrieve assets from Apple for their apps.

Operating an alternative app marketplace

Alternative app marketplaces can install and support software on iOS devices, access data across a catalog of apps, manage users' purchases and subscriptions, and more. They are responsible for meeting Notarization requirements, like all iOS apps.[5]

Operating an alternative app marketplace requires significant responsibility and oversight of the user experience, including content rules and moderation processes, anti-fraud measures to prevent scams, transparent data collection policies, and the ability to manage payment disputes and refunds.

Apple authorizes marketplace developers through the Alternative App Marketplace Entitlement (EU) to distribute a dedicated marketplace iOS app after meeting specific criteria and committing to ongoing requirements that help protect users and developers.[6]

Notarization for iOS apps

Notarization for iOS apps is a review that applies to all apps. It is focused on platform policies for security and privacy to maintain device integrity. Through a combination of automated checks and human review, Notarization 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.

Information from the Notarization process is also used for app installation sheets, which provide at-a-glance descriptions of apps and their functionality before users download them, including information about the developer, screenshots, and other essential information. Apps distributed on the App Store continue to be responsible for meeting Apple's high standards for user safety, security, and privacy and undergo the standard App Review process, including Notarization and enforcement of content and commerce policies.

Apple encrypts and signs all iOS apps intended for alternative distribution to ensure that users get apps from known parties.

Notarized apps also undergo a series of checks during installation to ensure that they haven't been tampered with and that the installation was initiated through an authorized alternative app marketplace.

---

5 For more details see https://developer.apple.com/support/alternative-app-marketplace-in-the-eu/ and https://developer.apple.com/documentation/marketplacekit.

6 For more details see https://developer.apple.com/support/alternative-app-marketplace-in-the-eu/.

If Apple determines that an iOS app contains known malware after it's been installed, it is prevented from launching and new installations are revoked.

Alternative distribution user experience

iOS 17.4 supports a new experience for app installation to help users authorize the installation of apps and alternative app marketplaces.

Users can install marketplace apps from a website owned by the marketplace developer after approving them with the Allow Marketplace from Developer control in Settings.

Before an app or marketplace app is installed, a new system sheet displays information developers have submitted to Apple for review, like the app name, developer name, app description, screenshots, and system age rating.

Users can manage their list of allowed marketplace developers and their marketplace apps in Settings and remove them at any time. Removing an allowed marketplace developer prevents new apps and updates from the developer's website from being installed. Deleting a marketplace app deletes all related data from the device and stops updates for apps from that marketplace, which may affect features and functionality for the apps installed from that marketplace.

Users can manage their default marketplace through a new default setting.

Browser Choice Screen in the EU

Apple has introduced a choice screen that provides users additional ways to choose a default web browser.

When users in the EU first open Safari on iOS 17.4, they are prompted to choose their default browser and presented with a list of the main web browsers available in their market to select as their default browser.[7]

Alternative web browser engines in the EU

Developers are able to use alternative browser engines — other than WebKit — for browser apps and apps providing in-app browsing experiences in the EU. iOS 17.4 introduces new capabilities to facilitate this change.[8]

---

7 For more details see https://developer.apple.com/support/browser-choice-screen/.

8 For more details see https://developer.apple.com/support/alternative-browser-engines/.

Developers must request and obtain the Web Browser Engine Entitlement (for browser apps that want to use alternative browser engines) or the Embedded Browser Engine Entitlement (for apps that provide in-app browsing experiences that want to use alternative browser engines).

As browser engines are constantly exposed to untrusted and potentially malicious content and can facilitate access to sensitive user data, they're one of the most common attack vectors for malicious actors. To help keep users safe online, Apple authorizes developers to implement alternative browser engines after meeting specific criteria and committing to ongoing functional, privacy and security requirements, including timely security updates to address emerging threats and vulnerabilities.

Default app controls for users in the EU

Apple has long made app visibilities and defaults available to users — including default controls for web browsing and mail apps.

Apple has introduced new default controls for users in Settings for:

- **App marketplace apps** — Users are able to manage their preferred default app marketplace through a new default setting for app marketplace apps. Platform features for finding and using apps like Spotlight are integrated with a user's default app marketplace.
- **Contactless payment apps** — Users are able to manage their preferred default contactless payments app through a new default setting, and can select any eligible app adopting the HCE Payments Entitlement as the default.

Users also have additional ways to manage their default browser setting. When iOS users in the EU first open Safari on iOS 17.4 or later, they're prompted to choose their default browser, and presented with a list of the main web browsers available in their market that can be selected as their default browser.

Apple also plans to introduce a new default control for users in Settings for navigation apps. Apple aims to make this solution available by March 2025.

Uninstallation of apps for users in the EU

Already today, Apple users have the ability to remove preinstalled apps from their Home Screen on iOS. Apple also plans to enable users to completely delete Safari from iOS, should they wish to do so. Apple aims to make this option available by the end of 2024.

Interoperability in the EU

Apple's interoperability efforts across software development kits and developer services, encompassing more than 250,000 APIs, enable developers to leverage the core technologies built into iOS and iPhone so users can access them right from developers' apps.

Apple is constantly expanding iOS interoperability. For example, in the European Economic Area, Apple has recently published its plan to introduce APIs for developers that support contactless payments for their wallet and banking apps, while protecting user security and privacy.[9] Developers will be able to offer these capabilities to users after the European Commission approves this plan.

Interoperability requests

Today, developers can ask questions or share feedback or suggestions to Apple in a variety of ways — such as developer support, the Apple Developer Forums, and Feedback Assistant. Apple has created a new dedicated process for developers to request additional effective interoperability with iOS and iPhone features.

Apple has introduced a new request form for developers to request additional effective interoperability with iPhone and iOS hardware and software features. Apple evaluates requests on a case-by-case basis to assess whether they appear to fall in scope of Article 6(7) DMA and, if so, Apple designs an effective interoperability solution if one can be supported, and lets the developer know if one cannot. New forms of access require Apple to engineer new APIs that will be delivered in future updates to Apple's operating systems. Developers can continue to use existing developer channels to ask questions and share feedback or suggestions about Apple's developer tools and services.[10]

Developers can submit requests for additional interoperability through a form available at: https://developer.apple.com/contact/request/interoperability/.[11]

---

9 For more details on Apple's plans see https://developer.apple.com/support/hce-payment-transactions-in-payment-apps/. The details are subject to approval by the European Commission.

10 For more details see https://developer.apple.com/support/ios-interoperability/.

11 For more details see https://developer.apple.com/support/ios-interoperability/.

Apple carefully reviews every submission, following a consistent and thorough process that includes the following steps:

- **Initial assessment.** Apple makes an initial assessment of the request, and based on the available information, determines whether the request appears to fall within the scope of Article 6(7) DMA.
- **Tentative project plan**. Based on Apple's initial assessment of the appropriateness of the request and whether it appears to fall within Article 6(7) DMA, Apple starts working on designing a solution for effective interoperability with the requested feature. Apple considers multiple factors when designing effective interoperability solutions. The integrity of iOS is always among the most important considerations. If appropriate, Apple aims to create a tentative project plan following the initial assessment.
- **Development and release of the interoperability solution.** To the extent an effective interoperability solution is feasible and appropriate under the DMA, Apple subsequently develops the solution. Development is highly specific to each request.

Alternative payments on the App Store in the EU

Alternative payment service providers and link out to purchase are available to developers for their apps distributed on the App Store in the EU. For their EU apps available on the App Store across Apple's operating systems, including iOS, iPadOS, macOS, tvOS, and watchOS, developers have additional payment options to offer digital goods and services:[12]

- **Payment Service Providers (PSPs)** — where developers use an alternative payment processor that lets users complete transactions within their app.
- **Linking out to purchase** — where developers direct users to complete a transaction for digital goods and services on their external webpage.

To use these new payment options, developers need to use the StoreKit External Purchase Entitlement, the StoreKit External Purchase Link Entitlement, or both. These new payment options are governed by the Alternative EU Terms Addendum.[13]

Using alternative PSPs and link out to purchase can create new threats to user security and privacy and may compromise the user experience. It's important for developers considering use of alternative PSPs and link out to understand that some OS or App Store features may not work as users expect. Helpful App Store features — like Report a

---

[12] For more details see https://developer.apple.com/support/apps-using-alternative-payment-providers-in-the-eu/.

[13] For more details see https://developer.apple.com/support/dma-and-apps-in-the-eu/#distribution-eu.

Problem, Family Sharing, and Ask to Buy — do not reflect these transactions. Users may have to share their payment information with additional parties, creating more opportunities for bad actors to steal sensitive financial information. And on the App Store, users' purchase history and subscription management only reflect transactions made using the App Store's In-App Purchase system. Apple has less ability to support or refund customers encountering issues, scams, or fraud. Developers who use alternative payments are also responsible for managing payment or billing issues, taxes, and other features currently supported by the App Store's system.

Developers distributing apps through App Store storefronts in the EU can now use either Apple's IAP or alternative payment processing to make digital goods and services available for purchase.

User experience for alternative payment service providers and link out to purchase

To help users understand whether an app contains an alternative payment option, the App Store displays an informational banner on the app's product page to identify the developer's enablement of this entitlement. When downloading an app, users are also informed if an app uses PSPs or link out on the purchase confirmation sheet. Apps that contain an alternative payment option are required to present users with a disclosure prior to each transaction or link out to purchase to help them understand that they are not transacting with Apple.

Commission and sales reporting

Developers who support PSPs and/or link out to purchase are responsible for paying a commission to Apple on the sale of digital goods and services on the App Store. Developers are required to report transactions to Apple for invoicing purposes using new APIs Apple provides.

For apps on iPadOS, macOS, tvOS, and watchOS, developers who use alternative PSPs get a 3% discount on the commission they owe to Apple. For linking out, the commission applies to sales of digital goods or services that are initiated within seven calendar days after the user taps "Continue" on the in-app notice sheet. This includes any adjustments for refunds, reversals and chargebacks.[14]

Requirements when using an alternative PSP within an app

A developer needs to use required StoreKit External Purchase APIs and follow usage requirements designed to help protect people's privacy and security, prevent scams and fraudulent activity, and maintain the overall quality of the user experience. In addition, when using an alternative payment processor within the app, it displays a system

[14] For more details see https://developer.apple.com/support/apps-using-alternative-payment-providers-in-the-eu/.

disclosure sheet to customers explaining that purchases are made through a source other than Apple.[15]

Requirements for linking out to the developer's webpage to complete a transaction for digital goods and services

Developers need to follow usage requirements designed to help protect people's privacy and security, prevent scams and fraudulent activity, and maintain the overall quality of the user experience.

For example, the link developers provide in an app must:

- Go directly to the developer's webpage without any redirect or intermediate links or landing page.
- Not pass additional parameters in the URL in order to protect the user (for example, their privacy).[16]

Expanded developer app analytics

Developers have long had access to dashboards and reports, providing valuable insights to help measure their apps' performance through App Analytics, Sales and Trends, and Payments and Financial Reports. Apple has expanded the analytics available for developers' apps both in the EU and around the world to help developers obtain even more insight into their businesses and their apps' performance.[17]

Over 50 new reports are available through the App Store Connect API to help developers analyze their app performance and find opportunities for improvement with more metrics in areas like:

- **Engagement** — with additional information on the number of users on the App Store interacting with a developer's app or sharing it with others.
- **Commerce** — with additional information on downloads, sales and proceeds, pre-orders, and transactions made with the App Store's secure In-App Purchase system.
- **App usage** — with additional information on crashes, active devices, installs, app deletions, and more.
- **Frameworks usage** — with additional information on an app's interaction with OS capabilities such as PhotoPicker, Widgets, and CarPlay.

---

15 For more details see https://developer.apple.com/support/apps-using-alternative-payment-providers-in-the-eu/.

16 For more details see https://developer.apple.com/support/apps-using-alternative-payment-providers-in-the-eu/.

17 For more details see https://developer.apple.com/support/dma-and-apps-in-the-eu/#app-analytics.

Apple is introducing a new App Store Connect API called the Analytics Reports API to provide access to reports on a continuously updated basis that include data from the App Store and iOS. Developers also have the ability to provide third-party access to their reports using the new API.

Users around the world could already choose if they wanted to share diagnostics and usage data that is generated by their iPhone use with Apple and developers. Apple has now implemented a single toggle, by which users are able to choose to share data with Apple and developers. Users still also have the option not to share this data at all. To protect the privacy of Apple users, Apple is also continuing to apply privacy measures to help ensure that users are not identifiable at an individual level.

Developers can continue to submit feedback or complaints related to Apple's data sharing tools via Feedback Assistant, which has now been updated to make it even more intuitive and transparent for developers to submit feedback or suggestions to Apple with regards to Apple's developer access tools – including potential requests for new data.

Apple plans to make further changes to its developer data access. Apple is also working on a secure solution for users to authorize developers to access data related to their users' personal data (to the extent it is available to Apple and users have consented to their personal data being shared with the developer). Apple aims to make this solution available by end of 2024.

User data portability tools for App Store account data

Apple's Data & Privacy site has been enhanced to provide users the ability to export their personal App Store data to authorized third parties. To help ensure that the intended uses of this sensitive user data meet user expectations, relevant third parties are responsible for meeting minimum eligibility requirements before they may access the Account Data Transfer API for requesting this data within their interfaces.

Users are able to schedule daily downloads of their App Store data for thirty days, or weekly downloads for one hundred and eighty days. The data provided is updated continuously and corresponds to the data available to Apple at any time following a user's request. New requests can be submitted once the scheduled downloads are completed. Users can review and revoke access to third parties at any time.

Apple plans to make further changes to its user data portability offering. Third parties offer migration solutions that help users transfer data between devices with different operating systems. To build on those options, Apple is developing a solution that helps mobile operating system providers develop more user-friendly solutions to transfer data from an

iPhone to a non-Apple phone. Apple aims to make this solution available by fall 2025. Apple is also creating a browser switching solution for exporting and importing relevant browser data into another browser on the same device. Apple aims to make this solution available by late 2024/early 2025.

Expanded safeguards on use of user and developer data

Data minimization is a foundational part of Apple's privacy-by-design philosophy. Wherever possible, users' personal data is processed and kept on the user's device and is not accessible to Apple. To build on that long-standing commitment, Apple is also taking the following measures:[18]

- **Streamlining data flows.** Where Apple identified cross-uses or combinations of personal data that would be prohibited by the DMA, it has ceased the use of App Store data in the context of other services and vice versa.
- **New policies and approval mechanisms.** Apple has put in place policies and approval mechanisms to ensure that any use of in-scope personal data complies with the DMA.

Apple has also reinforced its existing safeguards to prevent any misuse of non-publicly available data that is generated or provided by developers – such as expanded internal processes, additional policies, a new internal DMA audit process, and other additional approval mechanisms.

'Sign in with Apple'

Apple has revised its Guidelines[19] so that developers that use a third-party or social login service are not required to use or offer 'Sign in with Apple.' Apple only requires that users have a privacy-by-design option when signing in.[20] Developers can comply with this new rule by using 'Sign in with Apple' or a range of privacy-protecting third-party alternatives.

---

18 This applies to the extent personal data is accessible to Apple.

19 This is reflected in Guideline 4.8.

20 For more details see https://developer.apple.com/app-store/review/guidelines/#login-services.

Mediation

Already today, Apple has processes in place that help developers appeal decisions associated with their access to the App Store. Apple has also implemented a mediation process[21] for developers established in the EU who want to distribute apps on EU storefronts of the App Store, and are not satisfied that Apple correctly applied the terms relating to the access to the App Store in their specific case. The mediation is available following a developer's unsuccessful appeal to the App Review Board. It is EU-based, easily accessible, impartial, independent, and free-of-charge.

Compliance Function

Apple has established a dedicated internal DMA Compliance Function and appointed a Head of DMA Compliance Function and a DMA Compliance Officer.[22] Apple is committed to conducting business ethically, honestly, and in full compliance with applicable laws and regulations, including the DMA.

Other DMA areas

There are a number of other areas relevant to the DMA where Apple's existing business practices were already in compliance with the DMA's requirements. This concerns Articles 5(3), 5(6), 5(8), 6(5), 6(6) and 6(13) DMA. That includes our strong commitment to conducting business ethically and honestly. Apple's external Ethics and Compliance website[23] and Global Whistleblowing Policy[24] are but two examples of this unwavering commitment, which goes above and beyond the DMA's requirements.

---

21 For more details see https://www.cedr.com/.

22 See Article 28 DMA.

23 For more details see https://www.apple.com/compliance/ and https://secure.ethicspoint.com/domain/media/en/gui/48987/index.html.

24 For more details see https://www.apple.com/compliance/pdfs/Apple-Global-Whistleblowing-Policy.pdf.