Apple's Non-Confidential Summary of DMA Compliance Report

iOS, iPadOS, 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 iPadOS, and to support users impacted by issues with apps downloaded outside of the App Store.

That's why Apple introduced protections — including Notarization for iOS and iPadOS 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 our commitment to iPhone and iPad, ensure iOS and iPadOS remain the safest mobile platforms users can choose, and that Apple's app ecosystem continues to offer all developers the greatest opportunity.

Developers can use these new options in the 27 EU member countries since Xcode 15.3, iOS 17.4, and iPadOS 18.

The European Commission has opened two non-compliance investigations related to iOS. Apple is engaged in ongoing constructive conversations with the European Commission to understand the concerns underpinning those investigations. Apple has already announced changes to its compliance plan to address stated concerns which are being implemented across iOS and iPadOS. Apple will reflect any resulting changes for iOS that stem from these investigations also for iPadOS, as applicable.[1]

[1] This report is a factual record of the measures Apple has put in place. It reflects Apple's accommodation of matters raised by the European Commission and is not a statement of Apple's legal position.

Alternative distribution on iOS and iPadOS in the EU

As of iOS 17.4 and iPadOS 18, developers are able to create alternative marketplace apps on iOS and iPadOS. Apple provides authorized marketplace developers access to new app marketplace frameworks and APIs that let them receive and retrieve notarized apps[2] 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 to notify users of any app updates, so users can be offered important functionality like automatic app updates.[3]

With iOS 17.5 and iPadOS 18, Apple also launched Web Distribution, which lets authorized developers distribute their iOS and iPadOS apps to EU users directly from a website owned by the developer.[4]

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 or directly through their website are set forth in the Alternative EU Terms Addendum.[5]

---

2 See more about notarized apps below.

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

4 For more details see https://developer.apple.com/support/web-distribution-eu/.

5 For more details see https://developer.apple.com/contact/request/download/alternate_eu_terms_addendum.pdf.

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.[6]

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 and iPadOS 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 and iPadOS apps.[7]

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 and/or iPadOS app after meeting specific criteria and committing to ongoing requirements that help protect users and developers.

Distributing directly from the developer's website

Web Distribution lets authorized developers distribute their iOS and iPadOS apps to EU users directly from a website owned by the developer. This option is available to EU users on devices running a minimum of iOS 17.5 or iPadOS 18.

---

6 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.

7 For more details see https://developer.apple.com/security/complying-with-the-dma.pdf.

Apple authorizes developers after meeting specific criteria and committing to ongoing requirements that help protect users. Authorized developers get access to APIs that facilitate the distribution of developer's apps from the web, integrate with system functionality, back up and restore users' apps, and more. Apps offered through Web Distribution must meet Notarization requirements to protect platform integrity, like all iOS and iPadOS apps, and can only be installed from a website domain that the developer has registered in App Store Connect.[8]

Using App Store Connect, developers can easily download signed binary assets and host them on their website for distribution. To install apps from a developer's website, users first need to approve the developer to install apps in Settings on their iPhone or iPad. When installing an app, a system sheet displays information that developers have submitted to Apple for review, like the app name, developer name, app description, screenshots, and system age rating.

Notarization for iOS and iPadOS apps

Notarization for iOS and iPadOS 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 helps 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 and iPadOS 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.

If Apple determines that an iOS or iPadOS app contains known malware after it's been installed, it is prevented from launching and new installations are revoked.[9]

---

8 For more details see https://developer.apple.com/support/web-distribution-eu/.

9 For more details about submitting an app for notarisation, see https://developer.apple.com/help/app-store-connect/distributing-apps-in-the-european-union/submit-for-notarization.

Alternative distribution user experience

iOS 17.4 and later, and iPadOS 18 and later, support an experience for app installation to help users authorize the installation of apps and alternative app marketplaces and understand more about apps before they download.

Users can install marketplace apps or apps from a website owned by the developer after approving them with the ‘Allow Marketplace from Developer’ or 'Allow Apps from Developer' controls 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 and later, 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. This capability is available to users in the 27 EU member countries and will be coming to iPadOS 18 later in 2024.[10]

Alternative web browser engines in the EU

To meet the DMA’s requirements, iOS and iPadOS developers are able to use alternative browser engines — other than WebKit — for dedicated browser apps and apps providing in-app browsing experiences in the EU.[11]

---

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

11 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). These capabilities are available to EU users on devices running a minimum of iOS 17.4 or iPadOS 18.

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.

In iOS 17.4 and later, Apple provides 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 apps** — Users are able to manage their preferred default contactless app through a new default setting, and can select any eligible app adopting the HCE **Entitlement** as the default.
- **Default browsers** — When opening Safari for the first time, users are prompted to choose their default browser from a browser choice screen. The screen displays a list of the main web browsers available in their market that can be selected as their default browser.[12]

The app marketplace default was introduced for iPadOS in September 2024. The default controls for browsers will come to iPadOS later in 2024.[13]

In addition, later in 2024, iOS and iPadOS will include the following updates in the EU to default app controls:

---

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

[13] As iPads do not have NFC radios, the contactless app default is not relevant to iPadOS.

- In a special segment at the top of iOS and iPadOS 18's new Apps settings, there will be a new Default Apps section in Settings where users can manage their default settings.
- In addition to setting their default browser, mail, app marketplace, and (on iOS only) contactless apps, users will be able to set defaults for phone calls, messaging, password managers, keyboards, and call spam filters.
- In spring 2025, Apple will add support for setting defaults for navigation apps and translation.

Uninstallation of apps for users in the EU

Apple users have the ability to remove preinstalled apps from their Home Screen on iOS and iPadOS. Additionally, in an update later in 2024, iOS and iPadOS will include the following updates to app deletion: the App Store, Messages, Camera, Photos, and Safari apps will be deletable for users in the EU. Only Settings and (on iOS) Phone will not be deletable.

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 /iPhone and iPadOS /iPad so users can access them right from developers' apps. Apple is constantly expanding iOS and iPadOS interoperability.

Interoperability requests

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 also provides a dedicated web form for developers to request additional effective interoperability with hardware and software features built into iOS, iPadOS, iPhone, and/or iPad.

Apple evaluates requests received on the web form 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.[14]

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

Apple announced new options for alternative payments on the App Store in the EU on January 25, 2024, which became available to developers on March 7, 2024.[15] On August 8, 2024, Apple announced changes to the ability of developers to communicate and promote offers available outside of the app from within the app for digital goods or services.[16] Apple is engaged in ongoing constructive conversations with the European Commission about those changes.

---

[14] For more details see https://developer.apple.com/support/ios-interoperability/.

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

[16] For more details see https://developer.apple.com/support/alternative-payment-options-on-the-app-store-in-the-eu/.

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 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.

Apple provides an App Store Connect API called the Analytics Reports API to provide access to reports that include data from the App Store, iOS, and iPadOS. Developers also have the ability to provide third-party access to their reports using the new API.

Users around the world can choose if they want to share diagnostics and usage data that is generated by their iPhone use with Apple and developers. Apple also provides 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 is also introducing 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.

---

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

User data portability tools for App Store account data

Apple's Data & Privacy page provides 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.

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 or iPad to a non-Apple phone or tablet. 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 later in 2024.

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 takes 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 does not use App Store data in the context of other services and vice versa.
- **New policies and approval mechanisms.** Apple provides policies and approval mechanisms to ensure that any use of in-scope personal data complies with the DMA.

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

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

‘Sign in with Apple’

Apple has revised its App Review 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.

Mediation

Apple has processes in place that help developers appeal decisions associated with their access to the App Store. Apple also provides 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 a dedicated internal DMA Compliance Function. It appointed a Head of DMA Compliance Function and DMA Compliance Officer, and has allocated additional dedicated employees to the DMA Compliance Function.[22] Apple is committed to conducting business ethically, honestly, and in full compliance with applicable laws and regulations, including the DMA.

---

19 This is reflected in Guideline 4.8. For more details see https://developer.apple.com/app-store/review/guidelines/.

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

21 For more details see https://www.apple.com/legal/dma/mediation/.

22 See Article 28 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 applicable requirements, even before the DMA applied to Apple. 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 and Global Whistleblowing Policy[23] are but two examples of this unwavering commitment, which goes above and beyond the DMA's requirements.

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