Non-Confidential Version

APPLE DISTRIBUTION INTERNATIONAL LIMITED

App Store –
Second Report on Risk Assessment and Risk Mitigation Measures
pursuant to
Articles 33, 34 and 35 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)

27 August 2024

App Store – Report on Risk Assessment and Risk Mitigation Measures

OVERVIEW

This Risk Assessment Report is structured as follows:

Section 1 contains an explanation of Apple's approach to its second DSA App Store risk assessment and this report.

Section 2 describes the risk profile of the App Store, with reference to its key attributes and functionalities. It also describes certain attributes and functionalities that exist on other commonly used online platforms, including VLOPs, that do not exist on the App Store. This is intended to inform the assessment of the Systemic Risks and their risk mitigation measures, which is detailed in Section 3.

Section 3 contains the results of Apple's assessment of how the Systemic Risks in the EU may stem from the design, functionality or use of the App Store, as well as Apple's identification and assessment of its risk mitigation measures that address those risks.

Annex 1 (separate enclosure) contains background detail on App Store features, and relevant policies, procedures and controls.

*** *** *** *** ***

This Report was prepared by Apple Distribution International Ltd. ("ADI") solely for transmission to the European Commission and the Digital Services Coordinator for Ireland, *Coimisiún na Meán*, pursuant to Article 42(4)(a) and (b) of the DSA. The report is confidential and contains commercially sensitive information. It cannot be disclosed under Regulation 1049/2001 as this would undermine Apple's commercial interests, including its intellectual property. For the sake of completeness, Apple intends to publish a non-confidential version of the Report, in accordance with Article 42(4), following receipt of the second DSA audit report pursuant to Article 37(4).

SECTION 1: INTRODUCTION AND BACKGROUND

Section overview

This section of the report contains an explanation of Apple's[1] approach to its second App Store risk assessment and this report.

2024 Report and its structure

This report contains the results of the second Apple App Store risk assessment, which has been conducted in accordance with Article 34 of the DSA, as well as Apple's assessment of its App Store risk mitigation measures pursuant to Article 35 of the DSA. The report builds on the August 2023 App Store Risk Assessment (the "First App Store Risk Assessment"), which was submitted to the European Commission on 30 August 2023, and subsequently to *Coimisiún na Meán*. Unless stated otherwise, definitions from the First App Store Risk Assessment are adopted in this report.

This report relates to Apple's provision of the App Store service[2] in the EU, which the Commission designated in April 2023 as a single VLOP.[3]

Sections 1 and 2 of the First App Store Risk Assessment include background information on the App Store VLOP designation and Apple's risk assessment methodology. That detail is not repeated in this report, save where Apple has looked at different information sources in 2024 to inform its risk assessment work.

Section 3 of the First App Store Risk Assessment details certain relevant Apple-level (i.e. non-App Store specific) functions, policies and practices that apply to all of Apple's products and services across the wider Apple ecosystem. These protections apply to the use of all Apple devices, regardless of whether a user engages with the App Store, and, while not forming part of the design or function of the App Store itself, and the provision of the App Store by Apple, they contribute to the overall risk environment in which the App Store operates. These protections are not limited to, but extend to, Apple in relation to its provision

---

1 Although ADI is responsible for the provision of the App Store in the EU, and for determining the purposes and means of processing personal data in the context of this provision, and considering that ADI personnel contribute to the policies, processes and procedures relevant to the provision of the App Store in the EU and globally, for the purposes of this report, and unless otherwise stated, we do not distinguish between ADI and Apple Inc. Instead, we refer to "Apple" policies, processes and procedures, without prejudice to which entity is providing the actual service or product being discussed.

2 At the time of publication of the First App Store Risk Assessment, Apple operated five separate App Stores in the EU (iOS App Store, iPadOS App Store, watchOS App Store, macOS App Store, and tvOS App Store). Since then, Apple has launched a separate visionOS App Store for the Apple Vision Pro device in France and Germany.

3 ADI considers these services to be separate online platforms, which have significant material differences from both a developer and end user perspective. ADI considers that only iOS App Store should have been designated as a VLOP. Nonetheless, in the light of the definition of App Store in the Commission's decision, ADI has prepared this Report on the basis that it extends to iOS App Store, iPadOS App Store, watchOS App Store, macOS App Store, tvOS App Store, and the visionOS App Store. We refer to the "App Store" as referring to all of those services.

of the App Store. These controls are not detailed in the second App Store risk assessment, save to the extent that they materially mitigate any Systemic Risks that stem from the design, function or use of the App Store, and are referred to in Section 3.

Sections 4 and 6 of the First App Store Risk Assessment contain detailed background information on the operation of the App Store and the risk mitigation measures that Apple developed since it launched the App Store over 15 years ago. That detail was important to provide the background relevant to Apple's Article 34 assessment of the Systemic Risks and Apple's Article 35 risk mitigation measures assessment, particularly for the purposes of its first report. Rather than repeat that content this year, Apple has consolidated this information into Annex 1, which has been updated to reflect any material changes in the operation of the App Store and its risk mitigation measures since 28 August 2023.

Sections 5 and 7 of the First App Store Risk Assessment contain respectively Apple's assessment of the Systemic Risks and assessment of risk mitigation measures to assess those risks. In this 2024 report, those sections are consolidated into a new section 3, with some information presented in a table format.

The First App Store Risk Assessment was drafted as at 27 August 2023. Apple now has the benefit of data derived from additional controls and processes that it implemented to address its DSA obligations and additional reference points to take into account, such as the European Commission's Article 35 guidelines on the mitigation of systemic risks for electoral processes. Such information has been factored into the second App Store risk assessment and risk mitigation assessment, which covers the period 28 August 2023 to 27 August 2024.

Ongoing DSA engagement

In addition to its ongoing management of risks of the App Store, since submitting the First App Store Risk Assessment, Apple has actively participated in the following DSA related engagements:

1. Met with the European Commission to discuss the First App Store Risk Assessment and its ongoing DSA compliance efforts;
2. Received one RFI from the European Commission regarding the First App Store Risk Assessment ("ECRFI1"),[4] which it responded to in January 2024. Where relevant, information submitted to the Commission in its response has been incorporated into its ongoing risk assessment work;
3. Received an RFI from the European Commission regarding Article 40(12) of the DSA (researcher access to publicly accessible data),[5] which it responded to in February 2024.

---

[4] https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-apple-and-google-under-digital-services-act

[5] An RFI was sent to 17 VLOPs, including Apple. https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-17-very-large-online-platforms-and-search-engines-under

4. Monitored and considered requests for information issued to other VLOPs;
5. Provided the First App Store Risk Assessment to, and discussed it with, *Coimisiún na Meán*;
6. Engaged with the European Commission and other stakeholders in connection with the Commission's Article 35 guidelines on electoral processes, which included attending an in-person "stress test" event, the provision of information to the European Commission on elections readiness, and attending three additional online meetings in the leadup to and following the European Parliamentary elections;
7. Engaged with the European Commission on the protection of minors;
8. Engaged in European Commission consultations regarding various aspects of the DSA, including the draft transparency report delegated act and related templates;[6]
9. Engaged via trade associations regarding the European Commission's Article 28 guidelines consultation; and
10. Attended the June 2024 DSA Risk Assessment stakeholder event, organised by the Global Network Initiative and Digital Trust and Safety Partnership.

Feedback and additional insights on the conduct of DSA Risk Assessments from these engagements has been factored into the second risk assessment exercise.

DSA processes, systems and controls

As detailed in the First App Store Risk Assessment, Apple established a number of new processes, systems and controls in connection with its DSA obligations. These include:

1. Establishment of a dedicated DSA Compliance function. In the last 12 months the DSA Compliance function has:
    a. continued to develop DSA risk management and escalation processes, including processes to provide regular updates to the ADI Board, in conjunction with App Store Legal;
    b. developed a DSA training program for business functions that have a role in mitigating risks on the App Store; and
    c. engaged an audit firm in connection with, and organised and supervised activities relating to, the Year 1 DSA Audit.[7]

---

[6] Commission Implementing Regulation (EU) .../... of XXX laying down templates concerning the transparency reporting obligations of providers of intermediary services and of providers of online platforms under Regulation (EU) 2022/2065 of the European Parliament and of the Council / https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14027-Digital-Services-Act-transparency-reports-detailed-rules-and-templates- en

[7] The Year 1 DSA Audit refers to the independent audit that ADI is required to procure annually, pursuant to Article 37 of the DSA.

2. Creation of an enhanced illegal content reports portal ("Contents Report Portal")[8] and related systems to track and monitor notices and responses;
3. Establishment of transparency reporting processes. Apple has published two DSA App Store Transparency reports, since the First App Store Risk Assessment was finalised;[9]
4. Creation of a new DSA Legal webpage,[10] with various data points including points of contact information, a link to the Contents Reports Portal, Transparency reports and the Advertising repository.
5. The creation of a new process for DSA researcher data access requests; and
6. Establishing a process to obtain information from developers who are "traders" in the EU in order to comply with Article 30 of the DSA.

Internal stakeholder engagement

DSA Compliance and App Store Legal worked with various teams and business functions responsible for App Store policies, procedures and controls, to understand if and how the risk profile of the App Store and its risk mitigation efforts have changed / been tested over the last 12 months. This includes engagement with teams responsible for the following functions:

1. App Review
2. Recommender Systems
3. Apple Search Ads
4. Trust and Safety
5. Privacy Compliance

External stakeholder engagement

Apple routinely engages with external stakeholders in connection with the operation of its services, including via teams dedicated to external engagement and its Government Affairs personnel.

In addition, as described in the First App Store Risk Assessment, senior personnel within each function in the App Store (and who were consulted in connection with this risk assessment) are highly attuned to current events and external commentary affecting the App Store and their functions in particular. They take account of such events and commentary in making ongoing improvements to risk mitigation measures that they are responsible for. Teams across Apple conduct direct engagement with government bodies, NGOs, relevant trade bodies and interest groups, as well as the press. They are also aware of and responsible for considering concerns raised by the extensive App Store developer community and its users. Apple's support and engagement in initiatives such as Safer

[8] https://contentreports.apple.com

[9] DSA Transparency reports are available here: https://www.apple.com/legal/dsa/ie/. The third App Store DSA Transparency report will be published on 30 August 2024.

[10] https://www.apple.com/legal/dsa/ie/

Internet Day provide a broader platform for discussions across the EU with Government agencies, NGOs, trade associations, and the general public.

Concerns and issues raised have been considered as part of this year's risk assessment efforts.

Overall observations

As detailed above, Apple has continued to engage extensively on matters relating to the DSA in connection with the App Store since it finalised the First App Store Risk Assessment and the VLOP obligations came into effect. This includes direct engagement with the European Commission and *Coimisiún na Meán,* participation in a number of consultation processes, and active monitoring of issues highlighted in requests for information issued to and enforcement proceedings regarding other VLOPs. Despite its low election interference risk profile, Apple actively participated in the European Commission's elections interference stress test and follow-up stakeholder events. This engagement reinforced Apple's approach to the assessment of its risk profile and the adequacy of its risk mitigation measures.

Having now concluded its second assessment of the Systemic Risks and the adequacy of its risk mitigation measures, Apple is satisfied that the conclusions it reached as part of its First Risk Assessment are sound. Nothing in the intervening period has caused Apple to doubt the robustness of its First Risk Assessment or the adequacy of its risk mitigation measures. Apple actively monitors and manages the Systemic Risks and continues its considerable efforts to render the App Store a safe and trusted place for users to discover and download apps.

SECTION 2: APP STORE RISK PROFILE

Section overview

This section of the report describes the risk profile of the App Store, with reference to its key attributes and functionalities. It also describes certain attributes and functionalities that exist on other large online platforms, including VLOPs, that do not exist on the App Store.[11] This is intended to inform the ongoing assessment of the Systemic Risks and their risk mitigation measures, which are detailed in Section 3.

Core App Store attributes and functionalities

For DSA purposes, "recipients of the service" are:

1. Developers of apps; and
2. End users (also referred to as users).

Developers appoint ADI as their commissionaire for the marketing and delivery of apps to end users in the EU. Those end users are users of Apple devices who discover and download apps in the App Store in the EU.

The App Store operates 175 region-specific "storefronts", and users transact through a storefront based on their home country. Each EU Member State has a separate storefront. The App Store is available in 40 languages, including 17 official languages of the EU. Information presented in the App Store is therefore "localised", such that app metadata is displayed in different languages, depending on a user's location and language settings.

From its inception, the App Store was designed in such a way as to protect users of Apple devices by creating a safe and trusted environment offering a wide variety of curated apps. Every app and every app update submitted to the App Store is closely reviewed by both automated systems and human experts trained to review apps offered on the App Store for safety, user privacy and approved business models, such that they provide a good user experience. This pre-publication review already sets the App Store apart from other online platforms, where content can be posted without any prior checks. Post publication, apps are subject to ongoing monitoring and multiple controls to enable Apple to take action when it is alerted to problematic developers or apps.

App Store content types

As detailed in Annex 1, there are four types of content on the App Store that users can access, and therefore where, in principle, users could be exposed to illegal content and other risks. These content types are described below, as well as inherent design limitations, which feed into Apple's assessment of how the Systemic Risks could arise from the design, function and use of the App Store.

[11] For the avoidance of doubt, the risk profile of the App Store as described in the First App Store Risk Assessment has not changed. The information in this section is supplemental to the risk profile detail set out in that report.

In addition, we describe below how, in principle, users could be exposed to illegal or problematic content in connection with each content type. For the reasons described below, amongst the four content types on the App Store, the greatest risk of exposure to content giving rise to relevant risks arises in connection with apps and related product page information. As such, a key risk mitigation measure on the App Store is Apple's App Review process.

(a) Apps and related product page information

Worldwide, the App Store hosts approximately 1.8 million apps, which are available for download by users. Apps are recorded against different app "categories", which include books, business, music, navigation, games, entertainment, productivity and food and drink.

When a user taps on an app during discovery, they are taken to the app product page, which provides information about the app. Most of the information on the app product page is input by the developer, such as developer and app information; app icons, screenshots, and previews; a privacy policy URL; support links; an age rating; and data handling practices. App product pages also contain user ratings and reviews (see below).

All apps available on the App Store, including most of the information that appears on app product pages, have already been submitted to and approved by App Review. As detailed in Annex 1, App Review involves, in every case, an automated element and a human review element. A key differentiator with other types of online platforms, including social media platforms, is that all apps and app metadata have been subject to review prior to their publication on the online platform.

As described in the First App Store Risk Assessment, absent any risk mitigation measures, an app store could be used to disseminate certain categories of illegal content to users in the EU, including:

1. apps designed to disseminate illegal content or facilitate illegal behaviours, such as fraud, including "bait-and-switch" apps, or apps that are designed to undermine fundamental rights;
2. apps that infringe the intellectual property rights of others; and
3. apps that facilitate activities that are illegal in certain Member States (for example, certain types of real money gambling).

The First App Store Risk Assessment also referred to the risk that in-app content could be defamatory or intended to offend. Apple cannot monitor such content but instead requires developers to ensure that they have controls in place for users to report such content (see below).

(b) User ratings and reviews

User ratings and reviews are the only type of content on the App Store that can be generated by end users of the service.

Users can post a star rating of between 1 to 5 stars, a review "title" and the review itself. Users cannot post images or videos, such that risks arising on other online platforms such as "*deepfakes*" and other images that are offensive or discriminatory do not arise in user ratings and reviews on the App Store. When an end user edits their rating or review, the most recent change will display on the relevant product page. If a user submits a new rating or review, the existing review is replaced.

Developers are also able to post responses to user ratings and reviews. No posting of images or videos is possible.

As detailed in Annex 1, ratings and reviews are subject to terms and conditions (the AMS Terms) and pre- and post-publication controls, including pre-publication scanning and post-publication removal.

Ratings and reviews are not themselves "recommended" by the App Store recommender systems. Instead, consolidated ratings are an input to recommender systems that highlight or profile particular apps to users.

In principle, users could be exposed to illegal content posted by other users, although in practice, the primary risk regarding user ratings and reviews relate to fake reviews (although Apple has effective controls in place that are aimed at addressing this risk).

(c) App Store editorial content

App Store editorial content is drafted by human App Store editorial teams. App Store editorial teams create a curated catalogue of apps for each category in the Today tab (for example, original stories, tips, how-to guides, interviews, App of the Day, Game of the Day, Now Trending, Collections, Our Favourites, Get Started). For each curated category, the editorial teams determine whether to "pin" certain categories in designated vertical positions on the Today tab landing page.

From time to time, App Store editorial teams also write content about local events. For example, in connection with the European Parliamentary elections in June 2024, in close cooperation with the European Parliament, App Store editors published content with information for users about the elections,[12] including localized information about apps and news sources.

All App Store editorial content is subject to internal editorial guidelines.

In principle, users could be exposed to illegal and problematic content posted by App Store editors, although in practice the overall risk of this content type posing issues is very low, not least because of the small number of Apple personnel who are responsible for drafting content and the subject matter(s) they write about.

(d) Apple Search Ads

[12] See https://www.europarl.europa.eu/news/en/press-room/20240507IPR21413/weekly-election-highlights and https://apps.apple.com/be/story/id1745174009.

Apple Search Ads are the only type of advertising on the App Store.[13] Apple Search Ads provide a means for third-party developers to increase the visibility of their apps that are already distributed on the App Store.

Apple Search Ads placements are clearly distinguished from organic App Store placements and search results with a prominent "Ad" mark (language localised), and may include border and background shading demarcations. Tapping on the "Ad" mark designation displays an "About this Ad" sheet, which provides information about why the user has been shown that particular Apple Search Ad and what criteria, if any, were used to display the app campaign.

Apple Search Ads is an entirely optional service for developers, accessible through an separate account (an Apple Search Ads account), using a different web portal from App Store Connect.

Apple Search Ads differ from traditional forms of online advertising, that may be present on other large online platforms, in that only pre-approved apps can be advertised. Thus, there is no ability to advertise non-apps, including physical goods or services, on the App Store.

Apple Search Ads are subject to additional terms and conditions (beyond the DPLA and App Review Guidelines), which are actively enforced.

In practice, the risk profile for Apple Search Ads is largely the same as for apps, although there is a moderate risk that Apple Search Ads could advertise content to users that is illegal to advertise in their home country or region.

Locations where users encounter content on the App Store

(a) Today tab

The Today tab contains App Store Editorial content (see above) and "Top" charts (apps are selected for charts based on the most downloads in the App Store within approximately the past 24-hour period). Editorial content can be "personalized" based on e.g. purchase or download behaviour in the App Store.

(b) The "Games" and "Apps" tabs

The Games and Apps tabs on the App Store provide dedicated experiences for games and apps that inform and engage customers through recommendations on new releases and updates, videos, top charts, and handpicked collections and categories. For these tabs, all apps are selected based on algorithmic relevance, App Store Editorial curation, and top charts.

(c) Search tab

The App Store Search tab provides an additional way for customers to find apps, games, stories, categories, in-app purchases, and developers. Before a user enters a search, the

[13] [CONFIDENTIAL]

Search tab shows popular or trending queries in the "Discover" section, as well as a list of apps that a user may want to search for in the "Suggested" section. These apps are selected based on aggregate search behaviour from information curated by Apple's editors. In some cases, suggested queries may be personalized for users in the "Discover" section and apps may be personalized for users in the "Suggested" section, based on prior engagement in the App Store. In sum, the apps shown in Search before a search term is entered are selected based on algorithmic relevance, App Store Editorial curation, and top charts.

Searches use metadata from developers' product pages to deliver the most relevant results. The main parameters used for app ranking and discoverability are the relevance of text / titles, keywords, and descriptive categories provided in the app metadata; user engagement in the App Store, such as the number and quality of ratings and reviews; and application downloads. Date of launch in the App Store may also be considered for relevant searches.

Third party UGC

The First App Store Risk Assessment details at paragraphs 5.5.1 to 5.5.4 the limits of the App Store risk profile, and the scope of Apple's obligations under the DSA. In particular, it explains that where risks arise within the app itself, and therefore outside the App Store, that is the responsibility of the developer, some of which will be online platforms and VLOPs themselves.

Apple has also explained to the European Commission previously that UGC on third party apps is outside the scope of its content moderation obligations under the DSA. Apple has no means to enforce any rules it might seek to adopt in connection with live moderation of such UGC, as it does not control content within third-party apps. Apple cannot reasonably be expected to monitor and police UGC on third-party apps.[14] Pursuant to the App Store terms and conditions applicable to developers, including the App Review Guidelines, responsibility for moderating UGC on third party apps is clearly a matter for the developers of those apps. Additionally, any developers that are "intermediary services" under the DSA may have their own legal obligations with regard to content moderation of their apps. This includes several developers that themselves operate apps that have been designated as VLOPs.

Apple reasonably can, and does, however, maintain and enforce contractual obligations for developers that wish to have access to the App Store and wish to allow UGC on their apps. Pursuant to Guideline 1.2, apps with UGC or social networking services must include:

1. a method for filtering objectionable material from being posted to the app;
2. a mechanism to report offensive content and timely responses to concerns;
3. the ability to block abusive users from the service; and

[14] Indeed, Recital 30 of the DSA, for example, states "Nothing in this Regulation should be construed as an imposition of a general monitoring obligation or a general active fact -finding obligation, or as a general obligation for providers to take proactive measures in relation to illegal content." This is also reflected in Article 8 "No general monitoring or active fact finding obligations ".

4. published developer contact information.

Attributes and functionalities that do not apply to the App Store

To focus the risk profile of the App Store and to distinguish it from other large online platforms, including other VLOPs, it is important to note that the below common features or characterisations do not apply to the App Store:

It is not a social media platform or online marketplace for physical goods and services, a messaging service, a pornographic content service, an online chat or discussion service, or a file storage or sharing platform.

To the extent that developers can set up accounts as part of the Apple Developer Program, they are subject to checks and controls that significantly limit the risk of the creation of "fake" accounts.

It is not a service where users can share content anonymously with other users, save that users can post ratings and reviews using a nickname.

The following features do not exist on the App Store:

1. One to one end-user chat (whether encrypted or unencrypted). As such, risks to minors and other users that arise in connection with the use of private chat that are a feature of other online platforms do not arise on the App Store;
2. The ability to form closed or small groups of users. As such, risks that arise from the ability of users when they can form closed or small user groups, for example risks to minors or other vulnerable individuals, do not arise on the App Store;
3. The ability for users to livestream content. As such, risks that arise from the ability to livestream content, which often cannot be or is not moderated in real time, do not arise on the App Store;
4. The ability for users to post images or videos or engage in concerted content dissemination.

The App Store is not a general news service / information source (beyond containing information about apps, and some limited information regarding current events (for example, the 2024 Paris Olympics)). As such, any risks of "disinformation" on the App Store are in no way comparable to other online platforms that are used to disseminate news and other general factual information to the public.

SECTION 3: ASSESSMENT OF SYSTEMIC RISKS AND RISK MITIGATION MEASURES

Section overview

This Section contains the results of Apple's assessment of how the Systemic Risks in the EU may stem from the design, functionality or use of the App Store, as well as Apple's identification and assessment of risk mitigation measures that address those risks.

In the First App Store Risk Assessment Apple concluded that it did not identify any meaningful basis to distinguish risks stemming from the design and function of the App Store from risks stemming from its use. Apple also concluded that it did not identify any risks in the EU beyond or separate from those listed in Article 34(1) that might reasonably be said to stem from the design and function of the App Store, or its use, and that might reasonably be said to be systemic in nature. Nothing in the intervening 12 months has caused Apple to reach different conclusions.

Approach to assessing the Systemic Risks and their mitigation

In this report the results of Apple's assessment of each Systemic Risk and related risk mitigation measures are set out in table format at the end of this section.

For each Systemic Risk, the table contains:

1. **Inherent Risk**: Any risk that may stem from the design, functioning or use of an app store without reference to risk mitigation measures. This risk is directly linked to functionalities and attributes of the App Store, and recipients of the service, described in Section 2. This includes both the level of risk and a summary of the rationale for the classification.
2. **Risk Mitigation Measures**: Measures that are in place on the App Store that mitigate the inherent risk.
3. **Performance metrics and other risk indicators**: This lists the performance metrics and other risk indicators that Apple monitors to assess the level of residual risk.
4. **Residual Risk**: This records the level of risk after risk mitigation measures and the performance metrics and other risk indicators have been factored into the assessment.
5. **Observations regarding controls effectiveness**: This records Apple's observations on whether it considers its controls are effective in addressing the relevant risk.

Inherent risks and residual risks are categorized as low, medium or high. This reflects Apple's assessment of risk, factoring in: (a) the nature of the risk; (b) the probability of the risk occurring (improbable, probable, highly probable); and (c) the severity of the risk if it crystalises (low impact, moderate impact, high impact). Probability and severity determinations are then combined and reflected in the risk determinations set out in the tables below.

Article 34(2) factors

Pursuant to Article 34(2) first paragraph, Apple is required to take account of whether and how certain specified factors may influence any of the Systemic Risks.

(a) Recommender systems and other algorithms

Recital 84 of the DSA states that "*where the algorithmic amplification of information contributes to the Systemic Risks*", this should be reflected in VLOP's risk assessments.

Apple makes limited use of recommender and other algorithmic systems, but end users of the App Store do receive recommendations with respect to a selected and limited set of apps on the App Store that have already been approved through the App Review process. There is also a limited search function on the App Store, which allows users to search for App Review approved apps and content, and which operates by algorithmic means. Some content placement can be "*personalised*", but users are given the choice to disable personalised recommendations (except for Child Accounts,[15] where recommendations cannot be personalised).

Controls detailed in Annex 1 ensure that any impact of the App Store's use of recommender systems or other algorithmic systems on the Systemic Risks involves ample and specific risk mitigation; in particular, Apple is confident that its current controls regarding the operation of its recommender systems are such that those systems do not lead to the amplification of information or disinformation that contributes to the Systemic Risks.

Apple teams responsible for its recommender systems have confirmed that during the last twelve months Apple has maintained the controls set out in the First App Store Risk Assessment. As reflected in Annex 1, during the last 12 months Apple made changes to default personalization settings for users under the age of 18. Previously, for Child Accounts, personalization was set as "off"; now the default is set to "off" for Child Accounts and Teen Accounts.[16] Teen Account users can elect to set personalization requirements to "on". During the last 12 months Apple has also made modifications to restrict the types of content that will be personalized for Teen Accounts.

Content moderation systems

Apple has in place various content moderation systems on the App Store, which are detailed in Annex 1 and categorized in its DSA transparency reports. During the period covered by this report, Apple has maintained the content moderation systems detailed in the First App Store Risk Assessment.

Content moderation relating to published apps

Apple continually trains and enhances its automated tools to address new and emerging threats and to factor in learning from human-based decision-making, and enhances the processes used by and tools available to human app review specialists.

[15] "Child Accounts" refer to accounts for users under 13 years of age (or the equivalent minimum age of valid consent without required parental approval).

[16] "Teen Accounts" refer to accounts for users under 18 years of age (or the equivalent age of majority).

Content moderation relating to published ads

See further below regarding "Systems for selecting and presenting advertising".

Content moderation relating to user ratings and reviews as well as developer responses

Apple continues to train and enhance the systems it uses to identify problematic user ratings and reviews. In the last 12 months Apple has deployed enhancements in machine learning, automation, and the human review process to detect and remove problematic content. Apple has established on-going efforts using machine learning models to monitor new types of fraud in user reviews. Moderation tools have also been enhanced to improve efficiency and transparency, including impacted users notifications. Dedicated moderation resources are regularly reviewed to evaluate the timeliness and quality of Apple's removal processes, including operational process enhancement in removing illegal and unsafe content identified in user reviews.

(b) Applicable terms and conditions

Apple maintains comprehensive terms and conditions – applicable to both developers and end users – that address key risks facing the App Store, including the Systemic Risks. The terms and conditions provide Apple with a basis for taking prompt action in the event that a developer or end user misuses the App Store. Developers and users who object to such action have recourse to various complaints mechanisms.

Apple made changes to both the DPLA and the AMS Terms in response to its DSA obligations.

Based on its experience over the last 12 months, Apple remains confident that its terms and conditions provide it with a sound basis for taking action where necessary, against both developers and end users, to mitigate the impact of any Systemic Risks. This includes developer and end user account terminations, app rejections and takedowns, and the removal of user ratings and reviews. Both developers and end users have recourse to complaints and/or appeal mechanisms if they disagree with actions Apple takes against them.

(c) Systems for selecting and presenting advertising

Recital 88 provides that "*The advertising systems used by [VLOPs…] can also be a catalyser for the systemic risks"*.

As detailed in Section 2, the only advertising on the App Store is made possible by using Apple Search Ads. Use of Apple Search Ads is subject to controls and in any event do not contain any "new" advertising content; this is a system that developers can use to promote apps that have already been approved by App Review. As such, Apple does not consider that Apple Search Ads can to any meaningful extent be reasonably or objectively said to be a catalyser for the Systemic Risks.

Apple further notes that Recital 79 to the DSA suggests that the way in which VLOPs "*design their services is generally optimized to benefit their often advertising-driven business*

models and can cause societal concerns." Although certain VLOPs may design their services in this way, it is certainly not the case for the App Store, where Apple Search Ads only provides developers an opportunity to promote their apps and not to "advertise" additional content. The promoted apps have already been reviewed and approved for the App Store and are subject to further review to confirm that they are not in violation of the Apple Search Ads terms and conditions.

Apple now publishes its online Ads Repository, which is accessible here: https://adrepository.apple.com. This lists the Apple-delivered ads on the App Store in EU storefronts, as well as "Restricted Advertising", which lists both account suspensions as well as the Apple-delivered ads on the App Store that were removed from EU storefronts after publication, due to terms and conditions violations.

The Apple team responsible for Apple Search Ads have confirmed that during the last twelve months Apple has maintained the controls set out in the First App Store Risk Assessment.

Data-related practices of the provider

Apple's data-related practices are a central differentiator of the App Store, and the whole Apple ecosystem; Apple provides its customers with market-leading standards of protection of privacy, complying in full with applicable data protection and privacy laws.

This risk assessment, including the assessment of the Charter right to the protection of personal data below, addresses extensively all relevant privacy and data protection considerations.

Teams responsible for App Store data related practices have confirmed that the controls detailed in Annex 1 and the First App Store Risk Assessment remain in place.

Intentional manipulation of the App Store

Pursuant to Article 34(2) second paragraph, Apple is required to analyse how the Systemic Risks are influenced by intentional manipulation of the App Store.[17]

Malicious actors are constantly seeking to circumvent App Store risk mitigation measures so as to publish or promote apps on the App Store. Where relevant, particularly with respect to "illegal content", Apple has addressed and factored such intentional manipulation into its risk analysis.

The results of Apple's 2023 efforts to reduce the occurrence of fraud on the App Store are detailed in Apple's 2024 fraud prevention analysis.[18] In summary, it states that:

1. As digital threats have evolved in scope and complexity over the years, Apple has expanded its antifraud initiatives to address these challenges and help protect its users. Every day, teams across Apple monitor and investigate fraudulent activity on

[17] Recital 84 provides further context, which Apple has factored into its assessment.

[18] https://www.apple.com/newsroom/2024/05/app-store-stopped-over-7-billion-usd-in-potentially-fraudulent-transactions/

the App Store, and utilise sophisticated tools and technologies to weed out bad actors and help strengthen the App Store ecosystem.

2. From 2020 through 2023, Apple prevented a combined total of over $7 billion in potentially fraudulent transactions, including more than $1.8 billion in 2023 alone. In the same period, Apple blocked over 14 million stolen credit cards and more than 3.3 million accounts from transacting again.
3. In 2023, Apple:
    a. Terminated ca. 118,000 developer accounts for potentially fraudulent activity;
    b. Blocked ca. 91,000 fraudulent developer accounts from being created; and
    c. Deactivated ca. 374 million fraudulent customer accounts.

Regional or linguistic aspects

Pursuant to Article 34(2) third paragraph, Apple is also required to take into account specific regional or linguistic aspects, including any that are specific to a particular Member State, when assessing the Systemic Risks. Recital 84 provides that "*Where risks are localised or there are linguistic differences*", VLOPs should account for this in their risk assessments.

Apple does not consider that regional or linguistic aspects have a material impact on the Systemic Risks that might reasonably be argued to stem from the App Store, and has seen nothing during the course of the last 12 months to suggest the contrary. The App Store is available in 40 languages. While individual storefronts may address users in or with a connection to particular Member States, and while linguistic and local editorial coverage is provided across those regions and languages, the App Store service and risk mitigation measures are not substantively variegated across the EU, other than as may be required by law.

Performance metrics App Store uses to monitor systemic risks

[CONFIDENTIAL]

The "performance metrics" listed in the tables below refer to a range of metrics and information sources that Apple collects and monitors in connection with its ongoing management of the Systemic Risks to inform its assessment and management of the residual risks and the effectiveness of its listed risk mitigation measures. These include:

(a) App Review metrics

This includes app rejections and approvals, as well as appeals and reinstatement metrics. These metrics contribute to Apple's ongoing assessment of risk and the effectiveness of its

risk mitigation measures, particularly as they relate to App Review. These are published in non-DSA App Store transparency reports.[19]

(b) Content moderation metrics

This includes measures taken in connection in the EU with published apps, ratings and reviews and Apple Search Ads. These details are published in Apple's DSA Transparency reports. These metrics contribute to Apple's ongoing assessment of risk and the effectiveness of its risk mitigation measures.

(c) Article 9 orders, and non-DSA takedown notices

This includes Article 9 and non-DSA takedown notices. Apple tracks and monitors all such notices. It reports Article 9 orders in its DSA Transparency reports. During the period covered by this report, Apple received one Article 9 order. Apple considers the absence or low number of Article 9 and take down notices such orders to be a relevant metric in assessing risks on the App Store.

(d) Article 16 illegal content notices

This includes reports of alleged illegal content, via the Content Reports Portal. Apple tracks and monitors all Article 16 notices, both with respect to their substance and processing times, as part of its DSA compliance efforts. It also reports on such detail in its DSA Transparency reports. Again, these notices assist Apple in its ongoing assessment of risk and the effectiveness of its risk mitigation measures.

(e) External feedback and commentary

This includes, but is not limited to, any feedback that may be received directly from the European Commission and *Coimisiún na Meán*, civil society groups and researchers, as well as publicly available information about issues impacting the Systemic Risks and how they might arise in the EU, both on other platforms and the App Store.

By way of example, with respect to the Article 34(1)(c) Systemic Risk relating to actual or foreseeable negative effects on electoral processes, Apple has had reference to the European Commission's guidelines on elections interference, the European Commission's report on Russian disinformation campaigns,[20] news articles and reports regarding attempts to interfere in the European Parliamentary elections, publications from the European Parliament about such attempts, and information about risks and mitigation measures Apple learned during the election interference stakeholder events.

---

[19] Non-DSA App Store Transparency Reports and their supporting data are available here: https://www.apple.com/legal/more-resources/

[20] "Application of the risk management framework to Russian disinformation campaigns" European Commission, August 2023: https://op.europa.eu/en/publication-detail/-/publication/c1d645d0-42f5-11ee-a8b8-01aa75ed71a1/language-en

Article 34(1)(a) Illegal content

To consider "illegal content' in greater detail, the breakdown below is based on the "illegal content categories" Apple reports in its DSA transparency reports.[21]

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators[22]	Residual risk	Observations regarding controls effectiveness
Violates Intellectual Property Rights				
High – Developers could use the App Store to publish copycat apps, and/or use content, imagery etc. that violates the IP rights of third parties. Limited risk of users engaging in IP infringements via the App Store via ratings and reviews, including because no ability to post images or videos.	• DPLA, including sections 2.8 "Use of Apple Services", 3.3.3 D "Legal and Other Requirements", Schedule 1 section 6.3 "Termination". • App Review Guidelines, including 5.2 "Intellectual Property" and 5.2.1. • AMS Terms, including Submission Guidelines that state that users must not use the service to "*post any materials that (i) you do not have permission, right or license to use, or (ii) infringe on the rights of any third party*". • Apple Advertising Terms of Service, including section 6(g)(IX)(A) and (B). • App Review procedures. Here, and below, this refers to the entirety of the app review process and enforcement of the terms of the DPLA and App Review Guidelines, including human and automated review, and related escalation procedures. • Dedicated Content Disputes team. Here, and below, this refers to the team referred to in Annex 1. • Ratings and review moderation. Here, and below, this refers to ratings and review moderation referred to in Annex 1.	• App Review, Rejections, Takedowns and Appeals • Article 9 orders, and Article 16 notices • Content moderation metrics • External commentary and feedback	**Low**	IP infringing content is not permitted on the App Store. App Review procedures mitigate the risk of copycat apps and apps that infringe the IP rights of third parties being admitted to the store. Apple has also established a number of measures to enable it to respond to complaints regarding IP infringing content that is already published, including the dedicated Content Disputes team and responding to Article 16 notices. These processes provide complainants of IP rights violations with an effective remedy to bring such violations, if established, to an end. Apple has no reason to believe that its risk mitigation measures are anything other than proportionate and effective with respect to mitigating the risk of IP infringements. Taking into account the performance metrics and other risk indicators that

[21] Transparency reports are available here: https://www.apple.com/legal/dsa/ie/

[22] For the avoidance of doubt, reference to a metric in this column also includes the absence of such an indicator. For example, reference to "Article 9 notices" means that Apple will use the existence of any such notices, as well as their absence, as indicators in assessing Residual Risks.

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators[22]	Residual risk	Observations regarding controls effectiveness
	• Notice and action mechanisms. Here, and below, this refers to the various notice and action mechanisms referred to in Annex 1.			Apple has identified as being relevant to this risk, Apple has seen no material indication that such risks are crystallising, or there is material unmitigated, or inadequately mitigated, risk of this kind, in connection with the App Store. Apple is confident that its risk mitigation measures appropriately, proportionately and effectively address this risk.
Provides or facilitates an illegal service				
High - Developers could distribute apps on the App Store that facilitate scams and fraud and engaging in fraudulent payment practices, including bait and switch apps. Limited risk that users are exposed to fraud and scams or the facilitation of an illegal service in ratings and reviews. There is some risk that bots can misrepresent the quality of apps through fraudulent ratings and reviews. There is also risk that Apple Search Ads are used to advertise content that is illegal in a particular region.	• DPLA, including sections 2.8, 3.2 "Use of the Apple Software and Apple Services", and 3.3.3 D. • App Review Guidelines, including 5 "Legal". • AMS Terms, including Submission Guidelines that state that users must not use the service to "*post…unlawful…content*" and "*plan or engage in any illegal, fraudulent, or manipulative activity*". • Apple Advertising Terms of Service, including section 6(g)(IX)(B). • App Review procedures. • Ratings and review moderation. • Notice and action mechanisms.	• App Review, Rejections, Takedowns and Appeals • Article 9 orders, and Article 16 notices • Content moderation metrics • External commentary and feedback	**Low**	Apple employs industry best practices to safeguard Apple customers and prevent potentially fraudulent transactions, across its services, including the App Store. Apple's fraud mitigation tools include, but are not limited to, Two Factor Authentication, Fraud Screening, Hostile Fraud Screening, First Party Misuse Screening, and Account Takeover Detection. The results of Apple's 2023 anti-fraud efforts are detailed above. Apple Search Ads has comprehensive policies and procedures in place to minimize risk of developers posting prohibited advertising in a given region. Apple has no reason to believe that its risk mitigation measures are anything other than proportionate and effective with respect to mitigating the risk of facilitating an illegal service. Taking into account the performance metrics and other risk indicators that

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators[22]	Residual risk	Observations regarding controls effectiveness
				Apple has identified as being relevant to this risk, Apple has seen no material indication that such risks are crystallising, or there is material unmitigated, or inadequately mitigated, risk of this kind, in connection with the App Store. Apple is confident that its risk mitigation measures appropriately, proportionately and effectively address this risk. However, Apple has recognised that the introduction of alternative distribution methods in connection with the EU Digital Markets Act will result in the fragmentation of data it receives regarding activity on iOS apps; this will limit the data Apple can aggregate and analyse for the purposes of its fraud detection and monitoring controls for the App Store, and may over time undermine such controls.
Violates consumer protection or privacy law				
Medium (Consumer Protection) – Developers could provide misleading information to consumers via the App Store in product page information, including in relation to the functioning of the app, its content, and payment information. Also there is some risk of hidden advertising regarding apps, albeit falling far short of	• DPLA, including sections 3.2, and 3.3.3 D. • App Review Guidelines, including 2.3 "Accurate Metadata", and 2.3.1. • AMS Terms, including Submission Guidelines that state that users must not use the service to "*post, modify, or remove a rating or review in exchange for any kind of compensation or incentive*" and "*post a dishonest, abusive, harmful, misleading, or bad-faith rating or review, or a rating or review that is irrelevant to the Content being reviewed*" and *"plan or engage in any illegal, fraudulent, or manipulative activity"*.	• App Review, Rejections, Takedowns and Appeals • Article 9 orders, and Article 16 notices • Content moderation metrics • External commentary and feedback	**Low**	Illegal consumer information (i.e. false and misleading information) is not permitted on the App Store. The App Store is designed in such a way that developers are required to provide users with information about the operation of their apps. App Review has in place processes to mitigate the risk of apps having functionality that does not align with the apparent purpose of the app, including human review of every app, which assists identification of illegal

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators[22]	Residual risk	Observations regarding controls effectiveness
the level of risk associated with other platforms, such as with social media platforms where "influencer" related advertising risks arise. There is also a risk that users could provide fake ratings and reviews (including via bots) giving a misleading impression regarding apps. *Privacy law addressed below at pages 30-31 (right to protection of personal data).*	• Apple Advertising Terms of Service, including section 6(g)(XI)(B), and provisions in the Apple Advertising Policies that require claims to be substantiated and prohibits misleading content. • App Review procedures. • Ratings and review moderation. • Notice and action mechanisms. • DSA "trader" information (per Art. 30). • AppleCare Support.			content of this kind that automated screening alone might not detect. Apple-delivered ads using Apple Search Ads are marked on the App Store. Various complaints mechanisms enable users to complain about apps that do not operate as described. Apple has no reason to believe that its risk mitigation measures are anything other than proportionate and effective with respect to mitigating the risk of violations of consumer protection or privacy law. Taking into account the performance metrics and other risk indicators that Apple has identified as being relevant to this risk, Apple has seen no material indication that such risks are crystallising, or there is material unmitigated, or inadequately mitigated, risk of this kind, in connection with the App Store. Apple is confident that its risk mitigation measures appropriately, proportionately and effectively address this risk.
Child sexual abuse material (CSAM)				
High – Developers could use the App Store to disseminate apps that contain CSAM content / or post CSAM material to app product pages. The risk profile here is significantly lower risk than platforms that enable file	• DPLA, including sections 2.8 and 3.2 – see in particular prohibition on the creation or distribution of "*any content or activity that promotes child sexual exploitation or abuse*". And section 3.3.3 D. • App Review Guidelines, including 5. • AMS Terms, including Submission Guidelines.	• App Review, Rejections, Takedowns and Appeals • Article 9 orders, and Article 16 notices • Content moderation metrics	**Low**	Apple maintains comprehensive policies and procedures to address the limited risk of CSAM material being disseminated via the App Store. All Apps are subject to the App Review process, including both automated and human

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators[22]	Residual risk	Observations regarding controls effectiveness
sharing / one to one or closed group chat. Nonetheless, the severity of the consequences for affected persons if such risk were to crystallise is high. There is a more limited risk with respect to ratings and reviews on the App Store specifically, as users have no ability to post images or videos.	• Apple Advertising Terms of Service, including section 6(g). • App Review procedures. • Ratings and review moderation. • Notice and action mechanisms. • Child Safety Counsel / CSAM procedures.	• External commentary and feedback		review, which includes the review of product page imagery and app binary. Apple maintains dedicated child safety counsel to address allegations of CSAM content on the service. Apple has no reason to believe that its risk mitigation measures are anything other than proportionate and effective with respect to mitigating the risk of CSAM. Taking into account the performance metrics and other risk indicators that Apple has identified as being relevant to this risk, Apple has seen no material indication that such risks are crystallising, or there is material unmitigated, or inadequately mitigated, risk of this kind, in connection with the App Store. Apple is confident that its risk mitigation measures appropriately, proportionately and effectively address this risk.
Incites terrorism or violence				
Medium – Developers could distribute apps that are intended to incite terrorism or violence, or content in app product pages that incites terrorism or violence. Risk that ratings and reviews are used to incite terrorism or violence, but low compared	• DPLA, including section 2.8 and 3.2 - see in particular prohibition on the use of the App Store *"to threaten, incite, or promote violence, terrorism, or other serious harm"*. And section 3.3.3 D. • App Review Guidelines, including 1.1, 1.1.1 and 1.1.7. • AMS Terms, including Submission Guidelines. • Apple Advertising Terms of Service, including section 6(g); also prohibitions in Apple Advertising Policies on discriminatory and defamatory content. • App Review procedures.	• App Review, Rejections, Takedowns and Appeals • Article 9 orders, and Article 16 notices • Content moderation metrics • External commentary and feedback	**Low**	App Store maintains comprehensive policies and procedures to address the risk of the App Store being used to incite terrorism or violence, including App Review and notice and actions mechanisms. Such content is prohibited by the Guidelines. Apple has no reason to believe that its risk mitigation measures are anything other than proportionate and effective

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators[22]	Residual risk	Observations regarding controls effectiveness
with social media platforms given the nature of the content.	• Ratings and review moderation. • Notice and action mechanisms.			with respect to mitigating the risk of inciting terrorism or violence. Taking into account the performance metrics and other risk indicators that Apple has identified as being relevant to this risk, Apple has seen no material indication that such risks are crystallising, or there is material unmitigated, or inadequately mitigated, risk of this kind, in connection with the App Store. Apple is confident that its risk mitigation measures appropriately, proportionately and effectively address this risk.
Illegal hate speech				
Medium - Developers could use an app store to seek to distribute apps with the intended functionality and purpose of promoting illegal or harmful speech, or such speech could be included in app product page detail (written content / imagery). Developers could inaccurately describe apps in product page to mask this intention. Such risks of illegal hate speech do not arise from the use of the App Store in a manner or to an extent comparable with other online platforms with business models focusing on	• DPLA, including sections 2.8, 3.2, and 3.3.3 D. • App Review Guidelines, including 1.1 that provides that apps "*should not include content that is offensive, insensitive, upsetting, intended to disgust, in exceptionally poor taste, or just plain creepy*", 1.1.1 that prohibits apps that are "*defamatory, discriminatory, or-mean-spirited, including references or commentary about religion, race, sexual orientation, gender, national/ethnic origin, or other targeted groups, particularly if the app is likely to humiliate, intimidate, or harm a targeted individual or group*", and 1.1.7 that prohibits "*harmful concepts which capitalize or seek to profit on recent or current events, such as violent conflicts, terrorist attacks, and epidemics*". • AMS Terms, including Submission Guidelines. • Apple Advertising Terms of Service, including section 6(g). • App Review procedures. • Ratings and review moderation.	• App Review, Rejections, Takedowns and Appeals • Article 9 orders, and Article 16 notices • Content moderation metrics • External commentary and feedback	**Low**	Offensive, discriminatory and illegal content is not permitted on the App Store. All developer content on the App Store is subject to pre-publication review, include the app binary and app product page information. Ratings and reviews are subject to content moderation. Apple has no reason to believe that its risk mitigation measures are anything other than proportionate and effective with respect to mitigating the risk of illegal hate speech. Taking into account the performance metrics and other risk indicators that Apple has identified as being relevant to this risk, Apple has seen no material indication that such risks are crystallising, or there is material unmitigated, or inadequately mitigated, risk of this kind, in

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators[22]	Residual risk	Observations regarding controls effectiveness
widespread dissemination and rapid amplification of UGC. Also some risk that illegal or harmful speech could be posted in ratings and reviews. Risk is comparatively lower than on other platforms, such as social media platforms, or blogs.	• Notice and action mechanisms.			connection with the App Store. Apple is confident that its risk mitigation measures appropriately, proportionately and effectively address this risk.
Violates advertising law				
Medium – Apps could be promoted through Apple Search Ads which violate advertising law, including by advertising illegal content. Risk is comparatively lower than on other platforms, as the only advertising in connection with the App Store is through Apple Search Ads, which only features apps which are already approved through App Review and subject to existing controls. There is a more limited risk with respect to ratings and reviews on the App Store specifically.	• DPLA, including sections 2.8, and 3.2. • App Review Guidelines, including all relating to illegal content. • AMS Terms, including Submission Guidelines that state that users must not use the service to "*post or transmit spam, including but not limited to unsolicited or unauthorized advertising, promotional materials, or informational announcements*". • All Apple Search Ads terms and conditions. • App Review procedures. • ASA review processes. • Ratings and review moderation. • Notice and action mechanisms.	• App Review, Rejections, Takedowns and Appeals • Article 9 orders, and Article 16 notices • Content moderation metrics, including ASA takedowns and suspensions • External commentary and feedback	**Low**	Illegal content is not permitted on the App Store. All developer content on the App Store is subject to pre-publication review, include the app binary and app product page information. Apple Search Ads, a specialist team which includes legal counsel, specifically enforces policies which prohibit restricted advertising in different countries and regions in connection with advertising. Apple has no reason to believe that its risk mitigation measures are anything other than proportionate and effective with respect to mitigating the risk of advertising law violations. Taking into account the performance metrics and other risk indicators that Apple has identified as being relevant to this risk, Apple has seen no material indication that such risks are crystallising, or there is material unmitigated, or inadequately mitigated, risk of this kind, in

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators[22]	Residual risk	Observations regarding controls effectiveness
				connection with the App Store. Apple is confident that its risk mitigation measures appropriately, proportionately and effectively address this risk.
Other (this category enables users to report allegations of illegal content not covered by the specific categories listed above)				
Medium - The Commission's draft transparency report template contains a number of additional content categories, including animal welfare and non-consensual behaviour (non-consensual image sharing and online bullying), and self-harm. Risk that developers use the App Store to distribute other types of illegal content such as these, although risk is low compared with other platforms, such as e.g. social media platforms and online marketplaces.	• DPLA, including sections 2.8, 3.2, and 3.3.3 D. • App Review Guidelines, including all relating to illegal content. • AMS Terms, including Submission Guidelines. • Apple Advertising Terms of Service, including section 6(g). • App Review procedures. • ASA review processes. • Ratings and review moderation. • Notice and action mechanisms.	• App Review, Rejections, Takedowns and Appeals • Article 9 orders, and Article 16 notices • Content moderation metrics External commentary and feedback	**Low**	Apple maintains comprehensive policies and procedures that mitigate the risk of illegal content being distributed via the App Store, including pre- and post-publication controls. Apple has no reason to believe that its risk mitigation measures are anything other than proportionate and effective with respect to mitigating the risk of other illegal content. Taking into account the performance Taking into account the performance metrics and other risk indicators that Apple has identified as being relevant to this risk, Apple has seen no material indication that such risks are crystallising, or there is material unmitigated, or inadequately mitigated, risk of this kind, in connection with the App Store. Apple is confident that its risk mitigation measures appropriately, proportionately and effectively address this risk.

In the First App Store Risk Assessment, Apple concluded that its terms and conditions prohibiting the dissemination of illegal content are vigorously and fairly enforced; they provide a basis for Apple to take fair and predictable action against developers and users who do not comply with the rules, including the removal of apps and termination from the App Store; and Apple does in fact take such action, extending not only to criminal content, but to a wide range of other illegal content. As such, Apple concluded that these terms contribute to its assessment that its risk mitigation measures in

connection with illegal content risk reasonably, proportionately and effectively mitigate these risks in so far as they arise from the design, function or use of the App Store. This overall conclusion has not changed after considering each of the illegal content categories above.

Article 34(1)(b) Actual or foreseeable negative effects on the exercise of fundamental rights

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Residual risk	Observations regarding controls effectiveness
Actual or foreseeable negative effects on rights to human dignity and respect for private and family life, enshrined in Articles 1 and 7 of the Charter				
High – Developers could submit apps with relevant malign intent, or containing illicit app binary functionality, or lacking the controls required for apps of the relevant kind by the Guidelines. Also, for example, in the cases of CSAM (see above), so-called "revenge pornography", "deepfakes", etc. Risks to human dignity and private and family life have not arisen from the use of the App Store in a manner or to an extent comparable with other online platforms with business models focusing on widespread dissemination and rapid amplification of UGC. Some risk in ratings and reviews, although no ability to post images or videos, and no chat functionality.	• DPLA, including sections 2.8 "Use of Apple Services", and 3.2 "Use of the Apple Software and Apple Services". • App Review Guidelines, including 1.1 "Objectionable Content", 1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.1.7, 1.2 "User-Generated Content", 1.4 "Physical Harm", and 5 "Legal". • AMS Terms, including Submission Guidelines that state that users must not use the service to "*post objectionable, offensive, unlawful, deceptive, inaccurate, or harmful content*". • Apple Advertising Terms of Service, including section 6(g). • App Review procedures. • Ratings and review moderation. • Child Safety Counsel / CSAM procedures. • Notice and action mechanisms.	• App Review, Rejections, Takedowns and Appeals • Article 9 orders, and Article 16 notices • Content moderation metrics • External commentary and feedback	**Low**	In the First App Store Risk Assessment Apple concluded that its existing processes to consider and take action against apps that give rise to actual or foreseeable negative effects on rights to human dignity and respect for private and family life are reasonable, proportionate and effective. [CONFIDENTIAL] A range of apps on the App Store have AI features or can be used to generate AI imagery. In addition to the Guidelines applicable to all apps, those apps with user-generated content are subject to a range of controls, including the requirement to include a method for filtering objectionable material from being posted to the app, a mechanism to report offensive content and secure timely responses, the ability to block abusive users, and publication of contact information for the developer. Apple has no reason to believe that its risk mitigation measures

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Residual risk	Observations regarding controls effectiveness
				are anything other than proportionate and effective with respect to mitigating the risk of negative effects on human dignity and respect for family and private life. Taking into account the performance metrics and other risk indicators that Apple has identified as being relevant to this risk, Apple has seen no material indication that such risks are crystallising, or there is material unmitigated, or inadequately mitigated, risk of this kind, in connection with the App Store. Apple is confident that its risk mitigation measures appropriately, proportionately and effectively address this risk.
Actual or foreseeable negative effects on developers' and users' rights to the protection of personal data enshrined in Article 8 of the Charter				
High – Developers could use an app store to disseminate apps that collect and track users' personal data, either in a misleading or hidden manner, and without user consent. They can process such personal data in a manner that is detrimental to users. Separately, an app store could also undermine developers' and users' right to the protection of their personal data, including by tracking browsing and	• Apple Privacy Policy. • Apple Privacy Governance. • App Store & Privacy Notice. • DPLA, including section 3.3.3 D "Legal and Other Requirements" which specifies the requirement that developers and apps "*must comply with all applicable privacy and data collection laws and regulations with respect to any collection, use or disclosure of user or device data (e.g., a user's IP address, the name of the user's device, and any installed apps associated with a user*". • App Review Guidelines, including 5. • AMS Terms, including Submission Guidelines that state that users must not use the service to "*post personal, private or confidential information belonging to others*".	• App Review, Rejections, Takedowns and Appeals • Article 9 orders, and Article 16 notices • Content moderation metrics • External commentary and feedback		In the First App Store Risk Assessment Apple concluded that the effectiveness of its risk mitigation measures is ensured firstly by Apple's ongoing compliance with GDPR, and secondly by putting users firmly in control of the management of their own data when using the App Store. In accordance with Article 24 of the GDPR, the measures implemented by Apple take account of the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. These measures are subject to continuous review. Apple has no reason

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Residual risk	Observations regarding controls effectiveness
searching activities over the app store and over third party apps or websites, including for advertising purposes.	• Apple Advertising Terms of Service, and Apple Search Ads privacy-by-design practices. • App Review procedures. • Ratings and review moderation. • Notice and action mechanisms. • Data and Privacy Icon. • App Privacy Reports. • App Tracking Transparency Framework. • App Sandbox. • Personalisation practices.			to believe that its risk mitigation measures are anything other than proportionate and effective with respect to mitigating the risk of negative effects on the right to protection of personal data. Taking into account the performance metrics and other risk indicators that Apple has identified as being relevant to this risk, Apple has seen no material indication that such risks are crystallising, or there is material unmitigated, or inadequately mitigated, risk of this kind, in connection with the App Store. Apple is confident that its risk mitigation measures appropriately, proportionately and effectively address this risk.
Actual or foreseeable negative effects on the rights of developers and users to freedom of expression and freedom of information, including the freedom and pluralism of the media, under Article 11 of the Charter				
Medium - An app store could take an overly zealous or restrictive approach to approving or publishing apps, or make arbitrary decisions regarding content, including ratings and reviews. App stores are not media service platforms. News publishers disseminate news apps via app stores.	• DPLA: All developers are permitted to join the Apple developer program provided that they meet Apple's requirements, which are required to keep the App Store a safe and trusted place. • App Review Guidelines, including the Introduction that states clearly that Apple strongly supports all points of view being represented on the App Store, as long as the apps are respectful to users with differing opinions and the quality of the app experience is high. Apple notes that such is its commitment to pluralism of the media that it uniquely and exceptionally exempts professional political satirists and humourists from its prohibition in Guideline 1.1.1 on defamatory, discriminatory, or mean-	• App Review, Rejections, Takedowns and Appeals • Article 9 orders, and Article 16 notices • Content moderation metrics • External commentary and feedback	**Low**	In the First App Store Risk Assessment Apple concluded that a broad range of views and opinions from across the EU are available on the App Store. The App Store's risk mitigation measures balance the tension between freedom of expression and the need to keep users safe. A very broad range of media voices across the EU are present on the App Store. Apple is not aware of material concerns being raised in any quarter

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Residual risk	Observations regarding controls effectiveness
	spirited content, including references or commentary about religion, race, sexual orientation, gender, national / ethnic origin, or other targeted groups. • AMS Terms: Users are permitted to post ratings and reviews of apps they have downloaded, provided that they comply with the Submissions Guidelines, such restrictions being designed to keep the App Store a safe and trusted place for all. • Apple Search Ads terms and conditions: Developers are permitted to advertise their apps via Apple Search Ads, provided that they comply with the applicable terms and conditions, such restrictions being designed to keep the App Store a safe and trusted place for all. • App Review procedures, including procedures for developers to challenge App Review decisions. • Ratings and review moderation. • Notice and action mechanisms: When Apple receives government takedown requests targeted at the media apps or journalist content, they are addressed in accordance with the escalation procedures detailed in Annex 1. The App Store Legal team and other functions assess whether the app complies with the Guidelines, and whether the request is in accordance with local law (both as to substance as well as whether the agency has the authority to make the request). App Store Legal will in some instances consult with local counsel on the legality of the request. The App Store Legal team can also escalate requests to the ERB for consideration. If a request is in accordance with local law the media app may be removed from a local App Store Storefront. Requests that are not in accordance with local law would only be actioned if the app otherwise violated the Guidelines.			with respect to negative effects in the EU for media pluralism stemming from the App Store. In those circumstances, Apple has no reason to believe that its risk mitigation measures are anything other than proportionate and effective with respect to mitigating the risk of actual or foreseeable negative effects for the exercise of freedom of expression and information, and for media pluralism. Taking into account the performance metrics and other risk indicators that Apple has identified as being relevant to this risk, Apple has seen no material indication that such risks are crystallising, or there is material unmitigated, or inadequately mitigated, risk of this kind, in connection with the App Store. Apple is confident that its risk mitigation measures appropriately, proportionately and effectively address this risk.

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Residual risk	Observations regarding controls effectiveness
	• Issuing of statements of reason.			
The right to non-discrimination under Article 21 of the Charter				
Medium - Risk could manifest in inadvertent discrimination when conducting developer screening, App Review, or responding to notices and actions. Risks to the right to non-discrimination do not arise from the use of the App Store in a manner or to an extent comparable with other online platforms with business models focusing on widespread dissemination and rapid amplification of UGC.	• DPLA, including the Developer Code of Conduct that prohibits developers from engaging in discriminatory practices and notes that repeated manipulative or misleading behaviour will lead to their removal from the Apple Developer Program. • App Review Guidelines, including 1.1.1. • App Review procedures: Apps are admitted onto the App Store unless they violate the DPLA or App Review Guidelines. • AMS Terms, including the Submissions Guidelines that state that users must not use the service to "*post objectionable, offensive, unlawful, deceptive, inaccurate, or harmful content*". • Apple Advertising Terms of Service. • App Review procedures. • Ratings and review moderation. • Notice and action mechanisms. • Issuing of statements of reason.	• App Review, Rejections, Takedowns and Appeals • Article 9 orders, and Article 16 notices • Content moderation metrics • External commentary and feedback	**Low**	In the First App Store Risk Assessment, Apple stated that it is not aware of any concerns from developers or users that Apple discriminates against them when attempting to gain access to the App Developer Program. As regards App Store content, App Review scrutinises app metadata when submissions are made to the App Store and any content that is discriminatory, and therefore not in compliance with the Guidelines, will not be admitted to the App Store. In this regard, the fact that every app is subjected to human review as well as automated review is a powerful risk mitigant assisting Apple to identify problematic content that automated screening alone may not identify. Apple has no reason to believe that its risk mitigation measures are anything other than proportionate and effective with respect to mitigating the risk of discrimination. Taking into account the performance metrics and other risk indicators that Apple has identified as being relevant to this risk, Apple has seen no material indication that such risks are crystallising, or there is material unmitigated, or inadequately mitigated, risk of this kind, in connection with the

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Residual risk	Observations regarding controls effectiveness
				App Store. Apple is confident that its risk mitigation measures appropriately, proportionately and effectively address this risk.
Actual or foreseeable negative effects on the rights of the child enshrined in Article 24 of the Charter (addressing also the risk of negative effects in relation to the protection of minors, under Article 43(1)(d))				
High – The risk is high with respect to content (primarily apps) potentially available on the App Store. There are risks that minors are exposed to marketing, profiling and financial risks through apps with malign intent. There is a low risk with respect to Conduct Risks and Contact Risks[23] as identified by the OECD within the App Store, given its limited functionality (there is limited opportunity for exposure to hateful / harmful / illegal behaviour, and hateful, harmful and illegal encounters).	• DPLA, including all sections referred to above regarding illegal content and illegal use of the service, and section 2.4 of the Schedules 1, 2 and 3 that provides that the developer is responsible for determining and implementing any age ratings or parental advisory warnings required by the applicable government regulations, ratings board(s), service(s), or other organisations for any content offered in their app. These age rating determinations are considered during App Review. • App Review Guidelines, including the introductory section to the Guidelines reminds developers: "*We have lots of kids downloading lots of apps. Parental controls work great to protect kids, but you have to do your part too. So know that we're keeping an eye out for the kids.*", 1.3 "Kids Category", 2.3.8, and 5.1.4 "Privacy – Kids". • Apple Advertising Terms of Service. • App Review procedures. • Age Ratings. • Kids Category apps. • App Review Guidelines regarding UGC. • Ratings and review moderation.	• App Review, Rejections, Takedowns and Appeals • Article 9 orders, and Article 16 notices • Content moderation metrics • External commentary and feedback	**Low**	In the First App Store Risk Assessment Apple stated that the App Store is not a service that is directed at or predominantly used by minors. However, Apple recognises minors access apps available on the App Store and maintains controls to protect them. Apple has created device level controls, such as Screen Time and Ask to Buy, to give parents control over apps that their children can download and use on their devices. Even if parents chose not to use Screen Time and related controls, all apps on the App Store have already been subject to both automated and human based review and App Store content (including in-app purchase icons, screenshots and previews) is subject to the 4+ age rating requirement.

[23] OECD Revised Typology of Risks for Children in the Digital Environment considers "Content Risks", "Conduct Risks", "Contact Risks" and "Consumer Risks", as well as the following "cross-cutting risks": Privacy Risks, Advanced Technology Risks and Risks on Health & Wellbeing. https://www.oecd-ilibrary.org/science-and-technology/children-in-the-digital-environment_9b8f222e-en

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Residual risk	Observations regarding controls effectiveness
	• Notice and action mechanisms. • Screen time and parental controls. • Child Safety Counsel / CSAM procedures. • Personalisation practices and restrictions.			A very significant number of apps are rejected after App Review due to concerns relating to minors. Apple is confident that its comprehensive privacy controls for all users, and additional safeguards for children (including Apple IDs for children, Family Sharing, App Store safeguards and requirements, Screen Time use and content restrictions) are appropriate. Apple is mindful, in this regard, that the risk profile of the Apple Store is substantially lower than other in-scope platforms such as social media services, services that seek or offer validation, or which use children's data to create extensive profiles for advertising purposes. Apple offers numerous other protections that apply to children. In 2023, Apple stated that it would continue to monitor the EU BIK+ strategy, including the ongoing work relating to an EU code of conduct on age-appropriate design. Apple has done so. The Commission has since established a new Taskforce on Age Verification, which held its first meeting in January 2024. Apple is actively monitoring the work of the new taskforce and will collaborate with it as required, and is currently considering

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Residual risk	Observations regarding controls effectiveness
				the European Commission's Call for Evidence on Article 28 Guidance. Taking into account the performance metrics and other risk indicators that Apple has identified as being relevant to this risk, Apple has seen no material indication that such risks are crystallising, or there is material unmitigated, or inadequately mitigated, risk of this kind, in connection with the App Store. Apple is confident that its risk mitigation measures appropriately, proportionately and effectively address this risk.
High level of consumer protection, enshrined in Article 38 of the Charter				
The protection of consumers is a foundational principle of the App Store. In Apple's assessment, the collective effect of the risk mitigation measures detailed in Annex 1 is to ensure a high level of consumer protection for end users when they engage with the App Store, which is both reasonable and proportionate in light of the level of Systemic Risks which may stem from the design, function or use of the App Store. See also above regarding illegal content (consumer protection).				

Article 34(1)(c) Actual or foreseeable negative effects on civic discourse and electoral processes, and public security

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Residual risk	Observations regarding controls effectiveness
Actual or foreseeable negative effects on electoral processes				
Low - Risk that developers could use an app store to seek to distribute apps with the intended functionality and purpose of interfering	• DPLA, including sections 2.8 "Use of Apple Services", 3.2 "Use of the Apple Software and Apple Services", and 3.3.3 D "Legal and Other Requirements". • App Review Guidelines, including the Introduction to the Guidelines that clearly states Apple strongly supports all	• App Review, Rejections, Takedowns and Appeals	**Low**	In the First Risk Assessment, Apple concluded that it considers that, bearing in mind its low risk profile in this respect, the App Store risk mitigation measures are reasonable and

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Residual risk	Observations regarding controls effectiveness
with electoral processes and seek to distribute those apps via an app store. Developers could inaccurately describe apps in product page to mask this intention. Low risk of coordinated campaigns or manipulative behaviour to influence user ratings and reviews designed to interfere with electoral processes using bots. External commentary and research focus on risks arising on social media.	points of view being represented on the App Store, as long as the apps are respectful to users with differing opinions and the quality of the app experience is high. Any app including content or behaviour which violates Apple's policies or terms will be rejected. Guideline requirements detailed above that relate to illegal content and human dignity are also relevant here. • AMS Terms, including Submission Guidelines that state that users must not use the service to "*post or transmit spam, including but not limited to unsolicited or unauthorized advertising, promotional materials, or informational announcements*". • Apple Search Ads terms and conditions, including the prohibition on *Political Content*. • App Review procedures, including reinforced training and messaging during election periods, and resources regarding objectionable content regarding current events. • Notice and action mechanisms. • Editorial engagement with European Parliament regarding messaging on Editorial Pages. • Ratings and review moderation.	• Article 9 orders, and Article 16 notices • Content moderation metrics • External commentary and feedback • Engagement in 2024 EC / Commission stakeholder processes (pre- and post- EU Parliamentary elections) • Points of contact including for government officials and authorities during election periods		proportionate, and are capable of dealing effectively with any risks which may arise in connection with civic discourse and electoral processes. The prohibition on political advertising further mitigates this risk. Apple has no reason to believe that its risk mitigation measures are anything other than proportionate and effective with respect to mitigating the risk of negative effects on electoral processes. This conclusion is reinforced by Apple's election interference risk efforts since then, including in connection with the European Parliamentary elections in June 2024. Apple has seen no material indication that such risks are crystallising, or there is material unmitigated, or inadequately mitigated, risk of this kind, in connection with the App Store. Apple is confident that its risk mitigation measures appropriately, proportionately and effectively address this risk.
Actual or foreseeable negative effects on civic discourse and public security (including disinformation)				
Low – Risks to civic discourse do not arise from the use of the App Store in a manner or to an extent comparable with other online platforms with	• To the extent that public security considerations are taken to extend to risk mitigation measures to identify and address illegal content or illegal conduct, these are addressed in the terms and conditions, and applicable Guideline provisions listed above in respect of illegal	• App Review, Rejections, Takedowns and Appeals	**Low**	In the First App Store Risk Assessment, Apple concluded that risk mitigation measures Apple has in place provide it with ample basis to take action against threats to public security or civic

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Residual risk	Observations regarding controls effectiveness
business models focusing on widespread dissemination and rapid amplification of UGC. Risk that developers could use an app store to seek to distribute apps with the intended functionality and purpose of undermining public security, e.g. by disseminating extremist content. Developers could seek to distribute those apps via an app store and inaccurately describe apps in product page to mask this intention. Likelihood of user reviews and ratings being used to undermine public security is very low. Ratings and reviews cannot contain AI-generated or other images or videos and cannot be rapidly or widely disseminated on the App Store. Disinformation low risk on the App Store as it is not a news / information service. External commentary and research focus on risks arising on social media (see e.g. November 2023 Dublin riots).	content. Those Guidelines provisions listed above in respect of the rights to human dignity and respect for private and family life, and freedom of expression, are also relevant to negative effects on civic discourse and public security. • AMS Terms, including Submission Guidelines that state that users must not use the service to "*post or transmit spam, including but not limited to unsolicited or unauthorized advertising, promotional materials, or informational announcements*". • App Review procedures. • Notice and action mechanisms. • Ratings and review moderation.	• Article 9 orders, and Article 16 notices • Content moderation metrics • External commentary and feedback		discourse which may arise in connection with the App Store. Apple has no reason to believe that its risk mitigation measures are anything other than proportionate and effective with respect to mitigating the risk of negative effects on civic discourse and public security. Taking into account the performance metrics and other risk indicators that Apple has identified as being relevant to this risk, Apple has seen no material indication that such risks are crystallising, or there is material unmitigated, or inadequately mitigated, risk of this kind, in connection with the App Store. Apple is confident that its risk mitigation measures appropriately, proportionately and effectively address this risk.

Article 34(1)(d) Actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Residual risk	Observations regarding controls effectiveness
Actual or foreseeable negative effects on gender-based violence				
High - Developers could use an app store to seek to distribute apps with the intended functionality and purpose of promoting or encouraging gender-based violence, or such content could be included in app product page detail (written content / imagery). Developers could inaccurately describe apps in product page to mask this intention. This risk could also manifest in ratings and reviews. The absence of any ability for users to share images or videos in ratings and reviews is a significant mitigant in the App Store of risks of this kind that might arise with app stores more generally. No one-to-one chat functionality and no ability to share images or videos in ratings and reviews is a significant mitigant in the App store of risks of this kind that might arise with app stores more generally. App Store is	• DPLA, including sections 2.8 "Use of Apple Services", 3.2 "Use of the Apple Software and Apple Services", and 3.3.3 D "Legal and Other Requirements". • App Review Guidelines, including those referred to above that relate to illegal content and the right to human dignity, such as 1.1.1 and 1.1.2. • AMS Terms, including the Submissions Guidelines that state that users must not use the service to "*post objectionable, offensive, unlawful, deceptive, inaccurate, or harmful content*". • Apple Search Ads terms and conditions, including section 6(g). • App Review procedures. • Ratings and review moderation. • Notice and action mechanisms.	• App Review, Rejections, Takedowns and Appeals • Article 9 orders, and Article 16 notices • Content moderation metrics • External commentary and feedback	**Low**	In the First Risk Assessment, Apple concluded that its assessments regarding the effectiveness of its risk mitigation measures relating to, respectively, dissemination of illegal content and the rights to human dignity, apply equally in respect of the risk of actual or foreseeable negative effects on gender-based violence stemming from the design, function or use of the App Store. Apple has no reason to believe that its risk mitigation measures are anything other than proportionate and effective with respect to mitigating the risk of negative effects on gender-based violence. Taking into account the performance metrics and other risk indicators that Apple has identified as being relevant to this risk, Apple has seen no material indication that such risks are crystallising, or there is material unmitigated, or inadequately mitigated, risk of this kind, in connection with the App Store. Apple is confident that its risk mitigation measures appropriately, proportionately and effectively address this risk.

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Residual risk	Observations regarding controls effectiveness
not a pornographic or adult platform.				
Actual or foreseeable negative effects on public health and minors, serious negative consequences to a person's physical and mental well-being				
Medium - Risks to public and individual health do not arise from the use of the App Store in a manner or to an extent comparable with other online platforms with business models focusing on widespread dissemination and rapid amplification of UGC. The risk that user ratings or reviews of apps hosted on the App Store may produce negative effects on public health and physical and mental well- being is low, because there is no ability for users to share images and there is no chat functionality. *Risks to minors in connection with children's rights are addressed above.*	• DPLA, including sections 2.8, 3.2, and 3.3.3 D. • App Review Guidelines, including 1.4 that addresses app behaviour that risks physical harm; 1.4.1 specifically addresses "medical apps"; 1.4.2 specifically addresses "drug dosage calculators"; 1.4.3 specifically addresses apps that "encourage consumption of tobacco and vape products, illegal drugs or excessive amounts of alcohol"; 1.4.5 provides that apps "*should not urge customers to participate in activities (like bets, challenges, etc.) or use their devices in a way that risks physical harm to themselves or others*". • AMS Terms, including the Submissions Guidelines that state that users must not use the service to "*post objectionable, offensive, unlawful, deceptive, inaccurate, or harmful content*". • Apple Search Ads terms and conditions. • App Review procedures. • Ratings and review moderation. • Notice and action mechanisms. • Screen Time and other parental controls.	• App Review, Rejections, Takedowns and Appeals • Article 9 orders, and Article 16 notices • Content moderation metrics • External commentary and feedback	**Low**	In the First Risk Assessment, Apple concluded that its risk mitigation measures to provide it with sufficient means to take action against threats to public or individual health which may arise in connection with the App Store. Apple considered the heightened vulnerabilities of young users with regard to risks to individual health and well-being; it provides a number of controls and a support structure (for example parental controls) which specifically address these risks. Given the likely impact and prevalence of such risks, certain controls are set to "on" by default for children or are readily available to parents to facilitate the safety of children. Apple has no reason to believe that its risk mitigation measures are anything other than proportionate and effective with respect to mitigating the risk of negative effects on public health and to a person's physical and mental well-being. Taking into account the performance metrics and other risk indicators that Apple has identified as being relevant to this risk, Apple has seen no material indication that such risks are crystallising, or there is material

Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Residual risk	Observations regarding controls effectiveness
				unmitigated, or inadequately mitigated, risk of this kind, in connection with the App Store. Apple is confident that its risk mitigation measures appropriately, proportionately and effectively address this risk.

Annex 1 – Overview of App Store features and relevant policies, procedures and controls

Overview

This Annex provides an overview of the lifecycle of an app in the App Store – including app discovery, where users learn about and download apps. This Section also summarises the stages before app discovery: developer onboarding; app review; and recommender, advertising, and moderation systems that impact the presentation of apps and reviews to customers. This Section also addresses the App Store's notice and action mechanisms, which help to mitigate potential App Store risks, as well as external risks that are the responsibility of developers, and Apple's DSA Compliance function, website and its DSA transparency reports.

The App Store provides app discovery and distribution

Developers appoint ADI as their commissionaire for the marketing and delivery of apps to end users in the EU. Those end users are users of Apple devices who discover and download apps in the App Store, through one of the five landing pages (tabs) – "Today", "Games", "Apps", "Arcade", and "Search" – or by visiting the product page of an app.[1]

Below is an overview of how App Store discovery works from the end user's perspective, and where they encounter content in the App Store that could in principle engage the Systemic Risks.

The App Store operates 175 country- or region-specific "storefronts", and users transact through a storefront based on their home country. Each EU Member State has a separate storefront.[2] The App Store is available in 40 languages, including 17 official languages of the EU.[3] Information presented in the App Store is therefore "localised", such that app metadata[4] is displayed in different languages, depending on a user's location and language settings. Editorially curated content (described below) may vary, depending on a user's location.

The "Today" tab

The Today tab is the first page a user sees when they click on the App Store icon on their device. Apple considers this a "daily destination" with original stories from App Store editors, featuring exclusive premieres, new app releases, Apple's all-time favourite apps, an "App of the Day", a "Game of the Day", and more. It offers tips and how-to guides to help customers use apps in innovative ways, and showcases interviews with inspiring developers. Stories are selected based on curation by the App Store Editorial team, and they share Apple's perspective on apps and games and how they impact users' lives, using artwork, videos, and developer quotes to bring apps to life.

---

1 There is some variation between the tabs available on each App Store. The five tabs listed in this paragraph appear on the iOS and iPadOS App Stores.

2 For App Store availability in EU storefronts, see https://support.apple.com/en-us/HT204411

3 https://developer.apple.com/localization/

4 In this Report, app metadata comprises text (such as title, descriptions and keywords) and visuals (such as icon, screenshots and video) that are shown in the App Store.

App Store editors create a curated catalogue of apps for each category in the Today tab (for example, original stories, tips, how-to guides, interviews, App of the Day, Game of the Day, Now Trending, Collections, Our Favourites, Get Started). For each curated category, the Editorial team determines whether to "pin" certain categories in designated vertical positions on the Today tab landing page.

The Today tab also features "Top" charts, such as Top Free Games and Top Paid Games with various categories (AR Games, Indie Games, Action Games, Puzzle Games, Racing Games, Simulation Games); Top Free Apps and Top Paid Apps with various categories (Apple Watch Apps, Entertainment, Health & Fitness, Kids, Photo & Video, Productivity); Top Podcasting Apps; and Top Arcade Games. Apps are selected for charts based on the most downloads in the App Store within approximately the past 24-hour period.

App Store editors can also choose to have categories personalised for the user based on prior engagement (for example, purchase or download) behaviour in the App Store. If a story has been personalised, the Today tab would surface and order stories that are most relevant based on a user's purchase and download history. For example, personalised stories related to games may be surfaced as relevant to users who recently downloaded apps in the games category.

The "Games" and "Apps" tabs

The Games and Apps tabs on the App Store provide dedicated experiences for games and apps that inform and engage customers through recommendations on new releases and updates, videos, top charts, and handpicked collections and categories. For these tabs, all apps are selected based on algorithmic relevance, App Store Editorial curation, and top charts.

When considering apps to feature in these tabs, App Store editors look for high-quality apps across all categories, with a particular focus on new apps and apps with significant updates.

"Arcade" tab

The Arcade tab in the App Store features games which are made available as part of Apple's subscription service "Apple Arcade".

Search tab

The App Store Search tab provides an additional way for customers to find apps, games, stories, categories, in-app purchases, and developers. Before a user enters a search, the Search tab shows popular or trending queries in the "Discover" section, as well as a list of apps that a user may want to search for in the "Suggested" section. These apps are selected based on aggregate search behaviour from information curated by Apple's editors. In some cases, suggested queries may be personalised for users in the "Discover" section and apps may be personalised for users in the "Suggested" section, based on prior engagement in the App Store. In sum, the apps shown in Search before a search term is entered are selected based on algorithmic relevance, App Store Editorial curation, and top charts.

Searches use metadata from developers' product pages to deliver the most relevant results. The main parameters used for app ranking and discoverability are the relevance of text / titles, keywords, and descriptive categories provided in the app metadata; and user engagement in the App Store, such as the number and quality of ratings and reviews and

application downloads. Date of launch in the App Store may also be considered for relevant searches.

App product page

When a user taps on an app during discovery, they are taken to the app product page, which provides information about the app.

Most of the information on the app product page is input by the developer, such as developer and app information; app icons, screenshots, and previews; a privacy policy URL; support links; an age rating; and data handling practices. The App Store also provides customer rating and review information on the app product page. This is the only UGC on the App Store. If the user has downloaded the app, they see a link to the Report a Problem feature, which lets customers request a refund, report a quality issue, report a scam or fraud, or report offensive, illegal or abusive content.

Apple's paid app placement option on the App Store (Apple Search Ads)

Developers may also engage in paid promotion of their apps in the App Store through Apple Search Ads which provides a means for third-party developers to increase the visibility of their apps that are already distributed on the App Store. Through Apple Search Ads, apps may be displayed in the Today tab; the Search tab and Search Results; and in the product page while browsing.

Apple Search Ads placements are clearly distinguished from organic App Store placements and search results with a prominent "Ad" mark (language localised), and may include border and background shading demarcations. Tapping on the "Ad" mark designation displays an "About this Ad" sheet, which provides information about why the user has been shown that particular Apple Search Ad and what criteria, if any, were used to display the app campaign.

Apple Search Ads is a purely optional service for developers, accessible through an independent account (an Apple Search Ads account), using a different web portal from App Store Connect.[5] Apple Search Ads were made available to users in certain EU storefronts five years ago; more were added thereafter.[6] Today, Apple Search Ads are available to users in most EU storefronts,[7] though only a small percentage of App Store developers choose to promote their apps using Apple Search Ads. If developers choose to not use the Apple Search Ads service to promote their app, their app will still appear across the various available organic placements of the App Store, including within search results, just as it would if the developer had chosen to use Apple Search Ads for securing promoted placements. The two services and placement algorithms work separately from each other.

App Store processes and functions help to provide a safe and trusted place for customers to discover and download apps

The content below provides a summary of the App Store process from a developer perspective.

Developers are screened and must agree to terms and conditions

---

5 App Store connect is a developer tool where developers upload, submit, and manage their apps.

6 https://searchads.apple.com/countries-and-regions

7 Apple Search Ads is not available to users on the Bulgaria, Estonia, Latvia, Lithuania, Luxembourg, Malta, Slovakia, or Slovenia storefronts.

(i) Sanctions screening

Apple conducts sanctions screening for all developers who wish to join the Apple Developer Program. Developer names and contact details are run against government consolidated sanctions lists. Two types of sanctions screenings are conducted: one for individuals, based on information submitted in the Developer Information Page, and one for organisations, based on information submitted in the Enrolment Information page of the enrolment.

Where a sanctions report contains a positive hit and the developer challenges a positive sanctions determination, the Global Export Sanctions Compliance team will seek more information from the developer. They then factor that additional information into any final determination.

Apple also conducts ongoing sanctions monitoring to ensure that developers who are already admitted to the Apple Developer Program have not been added to a sanctions list.

(ii) Identity verification and screening

Before an app can be published in the App Store, a developer must register to enrol as an Apple Developer. A developer must sign in with an Apple ID with two-factor authentication, review and accept the latest terms of the Apple Developer Agreement,[8] and enter identity information. If the developer is enrolling via the Apple Developer app, they are asked to verify their identity with a driver's licence or government-issued photo ID.

Trust & Safety Developer Fraud conducts identity verification and other risk-based checking, in order to identify developers who, it considers, may be unlikely to comply with the Apple Developer Agreement (the "ADA") and DPLA. Apple uses submitted developer data as a secure hash to scan for and block developers attempting to register multiple accounts.

The World Wide Developer Relations team conducts a screening intended to prevent fraudulent developers from enrolling, including verifying developer identity, enrolment country, and financial information, as well as automated checks against existing and terminated developer accounts to ensure that bad actors (that is to say, developers who have previously committed or show indicators of intending to commit serious breaches of the ADA, DPLA or App Review Guidelines) and associates do not re-enter the program.

If a developer passes this round of screening, they can then execute the DPLA, and begin the multi-step process of submitting an app for distribution on the App Store.

(iii) Trader Traceability

Pursuant to Article 30(1) of the DSA, since February 2024 Apple also obtains information from developers who specify that they meet the definition of a "trader", including (a) the developer's name, address, telephone number and email address; (b) identification documents; (c) payment account details; (d) registration information; and (e) self-

[8] "Trusted Flaggers" are organisations designated under Article 19 of the DSA, which have particular expertise and competence for the purposes of detecting, identifying and notifying illegal content.

certification by the developer committing to only offer products or services that comply with applicable EU law. This detail is published on the trader's app product page.

General review practices

(i) App Review Guidelines

The Guidelines are the cornerstone of the App Review process. The preamble to the Guidelines notes that the guiding principle of the App Store is to provide a safe experience for users to get apps and a great opportunity for all developers to be successful. The App Review team evaluates all new apps and app updates to ensure compliance with the Guidelines.

Through application and enforcement of the Guidelines, the App Store aims to limit potential risks, including the Systemic Risks within its control. While Apple is unable to monitor or prevent content hosted within third-party apps, the Guidelines provide detailed, comprehensive and relevant requirements regarding developer's own risk mitigation responsibilities.

Particularly relevant to the DSA are Guidelines that:

a) Prohibit objectionable content;
b) Contain specific rules for apps with UGC;
c) Contain specific rules for apps in the Kids category;
d) Require developers to set appropriate age ratings; and
e) Require compliance with privacy, intellectual property, consumer protection and all other applicable laws, including the U.S. Federal Children's Online Privacy Protection Rule ("COPPA") and GDPR.

Below are summaries of some of these important Guidelines that play an important role in the App Store's risk mitigation measures.

(ii) Section 1: Specific app review practices for "Safety"

Section 1 of the Guidelines on Safety states that users expect to feel safe in installing an app from the App Store, and need to have confidence that the app will not contain upsetting or offensive content, damage their device, or cause physical harm.

In 2022, 92,598 apps were rejected for non-compliance with Section 1 of the Guidelines.[9] In 2023, 103,629 apps were rejected for non-compliance with this section.

(A) Objectionable content

Section 1.1 (Objectionable content) states that "Apps should not include content that is offensive, insensitive, upsetting, intended to disgust, in exceptionally poor taste." Among other things, this section prohibits apps that contain:

a) defamatory, discriminatory, or mean-spirited content;

b) portrayals of people being killed, tortured, or abused;

[9] App submissions may be rejected for non-compliance with one or more Guidelines.

c) content that encourages violence, or illegal or reckless use of weapons;

d) overtly sexual or pornographic material. This includes apps that may include pornography or be used to facilitate prostitution, or human trafficking and exploitation; or

e) harmful concepts which capitalise on current events.

(B) User-generated content

Section 1.2 (User-generated content) states that apps with UGC present particular challenges, ranging from intellectual property infringement to anonymous bullying. To prevent abuse, apps with UGC or social networking services must include:

a) a method for filtering objectionable material from being posted to the app;

b) a mechanism to report offensive content and timely responses to concerns;

c) the ability to block abusive users from the service; and

d) published developer contact information.

Section 1.2 also provides that apps with UGC or services that end up being used primarily for pornographic content, Chatroulette-style experiences, objectification of real people (for example "hot-or-not" voting), making physical threats, or bullying do not belong on the App Store and may be removed without notice.

(C) Kids category[10]

Section 1.3 (Kids category) provides that apps in the "Kids" category must not include links out of the app, purchasing opportunities, or other distractions to kids unless reserved for a designated area behind a "parental gate".[11] In addition to complying with privacy laws applicable to children, Kids Category apps may not send personally identifiable information or device information to third parties and should not include third-party analytics or third-party advertising. In limited cases, third-party analytics may be permitted provided that the services do not collect or transmit any identifiable information about children (such as name, date of birth, or email address), their location, or their devices. Any third-party contextual advertising services in Kids category apps must have publicly documented practices and policies for Kids Category apps that include human review of ad content for age appropriateness (and a link must be provided to such policies and practices when the app is submitted for App Review).

(D) Physical harm

Section 1.4 (Physical harm) warns that apps that present risks of physical harm may be rejected and, for example, prohibits apps that encourage:

---

[10] The Kids category on the App Store are apps specifically designed for children ages 11 and under. Developers places their apps in one of three age bands based on its primary audience: 5 and under, 6 to 8, or 9 to 11.

[11] A parental gate presents an adult-level task that must be completed in order to continue. The App Store provides developers with guidance regarding the creation of parental gates here: https://developer.apple.com/app-store/kids-apps/

a) Consumption of tobacco and vape products, illegal drugs, or excessive amounts of alcohol;

b) Drink-driving or other reckless behavior, such as excessive speed; or

c) Use of devices in a way that risks physical harm to users or others.

(iii) Section 2: Specific app review practices for "Performance"

Section 2.3 requires developers to ensure that all app metadata, including privacy information, their app description, screenshots, and previews accurately reflect the app's core experience.

Section 2.3.8 requires all app metadata, including apps and in-app purchase icons, screenshots, and previews to adhere to a 4+ age rating, even if the app is rated higher. By way of example, even if a developer's game includes violence, images on the App Store should not depict a gruesome death or a gun pointed at a specific character.

(iv) Section 5: Specific app review practices for "Legal"

Section 5 of the Guidelines states that apps must comply with all legal requirements in any location where developers make them available, and specifies that the developer is responsible for understanding and ensuring their app conforms with all local laws, including but not limited to intellectual property laws. In addition, Section 5 states that apps that solicit, promote, or encourage criminal or clearly reckless behaviour are unacceptable, and warns that in extreme cases, such as apps that are found to facilitate human trafficking and / or the exploitation of children, the appropriate authorities will be notified.

In 2022, 441,972 apps / app updates were rejected for non-compliance with Section 5 of the Guidelines. In 2023, 420,914 apps were rejected for non-compliance with this section.

(A) Privacy

Section 5.1 (Privacy) states that protecting user privacy is paramount in the Apple ecosystem, and developers must be careful when handling personal data to ensure compliance with, among other things, privacy best practices, applicable laws, the terms of the DPLA, and customer expectations.

(B) Data practices

Section 5.1.1 (Data Collection & Storage) provides that all apps must:

a) include a link to their privacy policy, which must comply with Section 5.1, in an easily accessible manner;

b) secure user consent for the collection of user or usage data;

c) provide an easily accessible and understandable way to withdraw consent;

d) only request access to data relevant to the core functionality of the app;

e) respect user permission settings;

f) allow app use without a login if the app does not rely on account-based features; and

g) not compile personal information without the user's explicit consent.

Section 5.1.2 (Data Use & Sharing) further requires that, unless explicitly permitted by law, all apps must:

a) not use, transmit, or share someone's personal data without first obtaining their permission;

b) obtain explicit permission via the App Tracking Transparency APIs to track their activity;

c) not repurpose data collected for a different purpose without additional user consent; and

d) not attempt to secretly build a user profile based on collected data.

(C) Health

Section 5.1.3 (Health and Health Research) states that health, fitness, and medical data are especially sensitive and sets out additional rules for apps with such a focus.

(D) Kids

Section 5.1.4 (Kids) has additional privacy and data requirements for children:

a) apps must comply with all children data protection laws (for example, COPPA and GDPR);

b) apps should not include third-party analytics / advertising if intended for kids;

c) use of terms like "For Kids" and "For Children" is reserved for the Kids Category; and

d) apps not in the Kids Category cannot imply the app is for children.

(E) Location services

Section 5.1.5 (Location Services) provides that use of location services in an app is only appropriate if:

a) directly relevant to the features and services provided by the app;

b) the purpose of location services has been explained to the user; and

c) the user has been notified and provided consent before the collection, transmission, or use of any location data.

(F) Intellectual property

Section 5.2 (Intellectual Property) requires developers to only include content in their app if they own it or are licensed or otherwise have permission to use it, and directs developers who believe that their intellectual property rights have been infringed by another developer

on the App Store to submit a claim via the App Store Content Dispute web form.[12] If the app features third-party trademarks or copyrighted content or lets users stream or download third-party content, the developer must provide with its app submission its authorisation to use such content.[13]

(G) Gaming, Gambling and Lotteries

Section 5.3 (Gaming, Gambling, and Lotteries) states that developers must fully vet their legal obligations everywhere their app is available. Among other requirements, apps used in connection with real money gaming or lotteries:

a) cannot use in-app purchase to purchase credit or currency;

b) must have necessary licensing and permissions where the app is used;

c) must be geo-restricted to those locations; and

d) must be free on the App Store.

(H) Developer Code of Conduct

Section 5.6 contains the Developer Code of Conduct. It requires developers to treat everyone with respect, including in responses to App Store reviews, customer support requests and dealings with Apple. The Code of Conduct prohibits harassment, discriminatory practices, intimidation, and bullying. Repeated manipulative, misleading, or fraudulent behaviour will result in removal from the Apple Developer Program. It further states that apps should never attempt to "rip off" customers, trick them into making unwanted purchases, force them to share unnecessary data, or engage in manipulative practices within or outside of the app. The Code of Conduct Section also states that:

a) developer and app information must be truthful, relevant, and current;

b) manipulating the customer experience (for example, charts, search, reviews, or app referrals) is not permitted; and

c) indications that customer expectations are not being met (for example, excessive customer complaints, negative reviews, and excessive refund requests) may result in termination.

<u>App review escalations and new and emerging issues</u>

During the App Review process, app reviewers may escalate issues to App Review specialist teams or other functional groups, as needed, to provide input, to work with developers on compliance issues, or to take action against problematic apps. New and emerging issues are often escalated in order to seek guidance on the appropriate path forward, including for example in response to specific events, [CONFIDENTIAL], or new technologies, [CONFIDENTIAL]. Below are the key groups involved in app escalations.

---

12 https://www.apple.com/legal/intellectual-property/dispute-forms/app-store/

13 https://developer.apple.com/app-store/review/

(i) App Review Compliance

This team tracks trends of misleading app concepts and signals, as well as app spam issues. An app reviewer may escalate an app to this team to investigate app behaviour, including whether behaviour has changed since an initial review, to determine whether the app exhibits fraudulent or misleading functionality, or to determine whether developer-hosted content violates the Guidelines. If there is a problem, this team will work with the developer to bring the app into compliance or remove the app from the App Store, if appropriate.

(ii) App Store Improvements/Technical Investigations

If an app reviewer identifies a need for a deeper analysis of the technical functionality of an app, they will escalate the issue to Technical Investigations. For example, this team investigates whether an app uses private APIs that may violate the Guidelines' privacy and data collection requirements. Based on the results of a Technical Investigation, the app reviewer may reject the app. Additionally, learnings collected during these investigations are applied to help develop and refine automated review tools, to determine if existing and future app submissions contain similar issues.

(iii) App Review Policy

If an app presents a new or unique issue that requires policy or Guideline interpretation, an app reviewer will escalate that issue to the App Review Policy team. This team investigates novel apps, evolving technologies, and current trends in apps, as well as highly sensitive and legal issues. This team regularly works with and seeks advice from other functional groups, [CONFIDENTIAL]. The App Review Policy team meets on a weekly basis and as needed to consider app policy escalations. The App Review Policy team drives the evolution of App Review's policy enforcement efforts and informs the ongoing development of internal policies and updates to the Guidelines.

(iv) Legal, privacy, government affairs, child safety, global security investigations & regional experts

As explained above, the App Review teams are educated on potential legal issues and risks, including on topics such as CSAM, illegal content, suppression of human rights, and misleading public health information. On a daily basis, App Review escalates app issues to senior management in App Review and the App Store Legal team. The App Store Legal team provides legal advice and coordinates with various other internal legal and regulatory teams (including EU-based teams) across Apple (for example, Privacy Compliance, Privacy Legal, EU Regulatory Legal, Human Rights, Child Safety, Global Security), as well as external counsel, for input and advice on complex issues presented by apps.

(v) ERB

The ERB is composed of senior leaders who have ultimate decision-making responsibility regarding access for apps to the App Store. The ERB meets regularly and receives updates and management information from various App Store functions, including App Review and App Store Legal. These updates detail information regarding App Review processing times and approval/rejection information, and new and emerging issues, including new and novel types of apps.

Where escalation issues cannot be resolved by the App Review team or the App Store Legal team, they are escalated to ERB. The ERB will then decide next steps, including app takedowns, further engagement, or an exploration of viable alternatives, as appropriate.

App review rejections, suspensions, terminations, appeals

The underlying philosophy of the App Review team is to work with developers to ensure apps are compliant with the Guidelines, as well as local legal and regulatory requirements.

If an app under review is in violation of the Guidelines, the team may reach out to the developer to work with them on remediation, unless for example the app is clearly fraudulent. If the app is rejected, the developer receives a message describing the reasons for an app rejection. The message identifies the Guideline that the app violates, describes the ways in which the guideline has been violated and provides next steps to help resolve the rejection, including access to additional resources. Developers may also request a call to discuss issues with an App Review specialist.

The App Review team may, depending on the severity of the issue, afford the developer 14 to 30 days to rectify an objectionable content issue (for example, by content-takedowns, or user blocking) before removing the app or taking additional measures. They may also require the developer to update their content moderation plan and confirm mitigation measures are in place to avoid recurring issues.

Developers can respond to the reviewer with a request for additional information or further discussion of the issues, or may dispute the findings.

App removals and developer terminations are the most severe measure to be undertaken in circumstances where remediation attempts have failed or are not an option, such as in circumstances where the app is fraudulent, or facilitates illegal activity.

As explained in the "After You Submit" section of the Guidelines, developers can dispute decisions of App Review regarding app rejections or developer terminations, via an appeals process, which is overseen by the App Review Board (the "ARB").[14] The ARB is composed of experienced App Review specialists who investigate claims asserted in an appeal, the history of the app and interactions with the developer, and seek input from specialised functions where appropriate.

Very few appeals are sustained, which tends to confirm the robust nature of app removal and developer termination decisions. For example, in 2022, Apple removed 186,195 apps from the App Store. Only 18,412 of those decisions were appealed, and 616 resulted in the app being restored.[15] Similarly, 428,487 developer accounts were terminated. Only 3,338

---

[14] https://developer.apple.com/app-store/review/ - see "Appeals". This page includes a link to a form for developers to submit appeals.

[15] As noted in the 2022 Transparency Report, most app removals that are appealed are removed from the App Store due to illegality or fraud. Consequently, most appeals from developers of such apps are rejected.

developer account terminations were appealed and, of those, 159 resulted in a restoration.[16] In 2023, Apple removed 116,117 apps from the App Store. 18,628 of the removals were appealed, and 322 resulted in the app being restored. During the same period, Apple terminated 117,843 developer accounts. 4,737 of the developer account terminations were appealed; of those, only 126 resulted in the restoration of the developer account.[17]

Ongoing monitoring

The App Review process does not stop once an app is approved and published on the App Store. This is necessary for a number of reasons:

a) Initial automated and human review cannot be expected to have a 100% success rate. Problematic app developers go to great effort to hide malicious functionality in their apps. As a result, sometimes malicious apps are published on the App Store, despite Apple's extensive risk mitigation measures.

b) Many apps contain content that changes over time. Developers of fraudulent apps sometimes introduce a switching mechanism that makes the app appear benign (like a simple game) during initial review but contains a trigger that can be switched post-approval to serve illicit or fraudulent content (i.e. "bait-and- switch"). In 2022, Apple blocked or removed 23,823 apps for bait-and-switch tactics. In 2023, Apple removed or rejected 40,000 apps from developers who engaged in bait-and-switch activity.

c) An approved app may also be found to have misrepresented its privacy policies and be illegally using personal information. An app might also evolve into a threat not inherent to its design. For example, a simple message board app that appears harmless on its face during App Review might later be used for illegal purposes.

Ongoing App Review through automated scans and other threat detection tools address the impact of a threat discovered post-approval. These tools help ensure that Apple can identify the developer, track malicious patterns by the same developer, identify similar patterns presented by other apps, and cut off distribution at a single source. Apple can directly communicate with the app developer and rapidly remove the app from the App Store if necessary.

Automated and human-based app review

The App Review process applies to both new apps and to updates to existing apps (for example, when an app introduces a new version, adds new features, extends to new platforms, or uses an additional Apple technology).

Every app or app update provided to the App Store for distribution is uploaded through App Store Connect, which is a developer tool where developers upload, submit, and manage their apps. Upon submission, the developer creates an app record, provides app metadata, along with the app name and description and other relevant information.[18] A complete set of metadata must be provided (i.e. if a submission includes "placeholder" text, it will be

16 https://www.apple.com/legal/more-resources/docs/2022-App-Store-Transparency-Report.pdf
17 https://www.apple.com/legal/more-resources/docs/2023-App-Store-Transparency-Report.pdf
18 https://developer.apple.com/support/terms/

rejected). Every app or app update submission is then reviewed by the App Review team, first via automated means and then by human app reviewers

Automated review

The App Review automated process includes static binary analysis, asset analysis, and runtime analysis via automated on-device install, launch, and exploration tests. The aim of these automated processes is to efficiently gather information that can be interpreted by machine learning algorithms and analysed for threats and signals (for example, the presence of malicious URLs or executable code) that provide relevant app information to the human review component. The automated review process also conducts checks [CONFIDENTIAL], and cross-references apps and developers against previously identified threats in the App Store ecosystem to better detect malicious actors, fraud, and other abuses.

For over a decade, using proprietary machine learning tools and technologies, the App Store has developed an internal corpus of information used to mitigate risks, such as previously identified threats, identified malicious apps and developers, suspicious keywords, malicious IP addresses and URLs. For example, malicious URL detection involves analysing URLs that have been previously flagged for illegal or harmful content or characteristics. By analysing information in new app submissions for similarities with previously identified information, the automated review component of the App Review process helps keep bad apps and actors from entering or re-entering the App Store.

Similarly, automated review interprets cached text and images, [CONFIDENTIAL], and identifies potential threats like executable code, which could be used to change app features or functionality after app review and approval.

The information gathered during automated review flags potential risks and provides useful signals and information to human app reviewers to evaluate in more detail. [CONFIDENTIAL] Finally, as explained in more detail below, automated processes continue after approval of apps that are available on the App Store, with automated detection and escalation mechanisms continuing to scan for potential threats.

Automated review capabilities are continually assessed for their performance and improved. The App Review team works with engineering teams and domain experts across Apple to identify trends flagged by human app reviewers, investigate spikes in reports relating to specific issues (e.g. via Report a Problem), assess novel threats, and the applicability of both established and emerging technologies to mitigate these threats. Multiple improvement efforts have historically been introduced each year.

There are more than 100,000 app submissions in an average week. In 2022, App Review reviewed 6,101,913 submissions (including app updates), of which over 25 % were rejected by the App Review team for various compliance issues.[20] In 2023, App Review reviewed 6,892,500 submissions (including app updates); again, over 25 % were rejected.[21] App

[19] [CONFIDENTIAL]

[20] https://www.apple.com/legal/more-resources/docs/2022-App-Store-Transparency-Report.pdf

[21] https://www.apple.com/legal/more-resources/docs/2023-App-Store-Transparency-Report.pdf

Review therefore serves an important function in mitigating risks, including potential Systemic Risks, in the App Store.

Human review

Every app and every app update undergo human review. During human review, app reviewers analyse the signals provided by automated systems and review the features and functionality of apps to ensure they are compatible with the App Store's systems and products, comply with the Guidelines, and do not give signs of potential deceptive, abusive, or otherwise harmful behaviour. If a reviewer detects a potential Guideline violation, they engage with the developer, reject the app or further escalate issues to specialists within the App Review team or to other functional groups, such as the App Store Legal team. If there are no Guideline violations, the app may be approved for publication in the App Store.

[CONFIDENTIAL]

Human Review builds on and complements automated review, since human app reviewers are often better positioned than automated tools to identify apps that risk physical harm, apps which are unreliable, or apps which otherwise pose concerns in ways that are not readily apparent to automated (static and dynamic) tools. As regards safeguarding user data and privacy, [CONFIDENTIAL] a human app reviewer is trained to assess [CONFIDENTIAL] are appropriate for the app's functionality. For example, a human app reviewer will likely decide that a calculator app does not need to request access to data and functionality like photos or the microphone. Similarly, app reviewers are trained to evaluate whether an app age rating is appropriate given the app's content and functionality, as well as whether apps with user-generated content have sufficient content moderation mechanisms to protect children or mitigate risks related to offensive content, harmful concepts, or public security.

The App Store review process is carried out by over 500 human app review experts, including over 170 individuals based in the EU, representing 81 languages across three time zones. Prior to reviewing any apps, new employees receive four to six weeks of intensive training regarding, inter alia, all components of the Guidelines, including screening for privacy and data issues, particularly for children; objectionable content; apps with user-generated content; and legal considerations.

The App Review teams are educated on potential legal issues and risks – including highly sensitive topics such as CSAM, real money gambling, illegal content, suppression of human rights, and misleading public health information – and the appropriate escalation paths. Apps are assigned to individuals for review based on their skills, qualifications and experience, including language capabilities, cultural sensitivities, and specialised training.

After initial training, new App Review personnel work is monitored and audited, and they receive regular performance feedback and specialised training, as appropriate. All app reviewers have ongoing support and internal resources, such as mentoring, coaching, access to app review processes and policies, and weekly and ad hoc meetings with managers. The work of human reviewers is audited and new and emerging issues feed into guidance updates and learning resources. The App Review team also monitors customer

and developer feedback to assess performance. Additionally, the App Review Business Excellence team performs quality control and audit to conduct root-cause analysis and make necessary improvements, whether to tools or performance management of reviewers.

The diverse App Review team tracks evolving risks in the EU and around the world, based on trends, language cues, global events, and other signals, all of which is used to continually update and train the automated and human review functions. App reviewers are kept up to date regarding new and evolving risks via coaching, access to practices and policies, and meetings referred to above.

When App Review discovers apps that contain illegal content, fraudulent or malicious content or behaviour, it adjusts the review process to prevent such apps from being approved in the future. If Apple discovers apps that have not sought to circumvent the App Store review process per se but that are exhibiting malicious or user-unfriendly behaviours after installation, Apple similarly adjusts its processes to prevent this from reoccurring. If Apple discovers new malware on its platforms, it adjusts its custom-written malware scanners to scan apps already on the App Store and detect such malware in the future.

Post-publication review

The App Review process continues even after an app is first published on the App Store. Developers are required to submit updates to their apps to the App Review team. This ensures that Apple's App Review function reviews apps throughout their entire lifecycle, and can identify new features and functionality that may not comply with the Guidelines. Furthermore, the App Store takes action against apps that exhibit malicious or other problematic behaviours after they have become available in the App Store. The App Store has a number of automated tools in place to detect malware on existing apps, that it runs at periodic intervals to capture content at different times. This includes tools to identify "bait-and-switch" apps, where apps available on the App Store change or add new functionality after approval by the App Review team. Once flagged by automation, these apps are re-reviewed by human app reviewers to evaluate whether intervention is needed.

App Store User-Generated Content Measures

The only UGC on the App Store is user-generated app ratings and reviews, which are subject to content moderation by the Trust and Safety Operations team who also moderate developers' responses to reviews. The Trust and Safety Operations team takes both preventative and responsive steps by way of mitigation of risks arising from UGC, which include the publication of false, illegal or harmful content, or fraudulent conduct that is designed to manipulate an app's rating ("Rating and Review" fraud). Without ratings and reviews moderation, misleading and fraudulent information would be spread on the App Store, which could lead users to download malicious apps.

A number of key process mitigations apply to user submission or ratings and reviews. In particular, ratings and reviews can only be submitted by registered users who have downloaded the relevant app. Furthermore, all user ratings and reviews are subject to a publication delay before being published on the App Store.

A number of monitoring processes are carried out to protect against fake or fraudulent reviews, including scanning for spam, profanity and foul language, and multiple duplicate or similar entries. Furthermore, Apple has a number of systemic block and monitoring

processes to moderate user ratings and reviews and developer responses, and takes action against users and developers who do not comply with applicable ratings and reviews terms and conditions.

Reviews can be sorted by helpfulness, rating, or recency. When ordering reviews by helpfulness, Apple considers the review's source, quality, thoroughness, and timeliness as well as how other customers have engaged with the review.

The Trust and Safety Operations team also reacts when it is alerted to potentially problematic ratings and reviews, or developer responses, via "Report a Concern". This functionality and related process is described in further detail below.

The Trust and Safety Operations team works with a variety of partner teams, including AppleCare, to continually improve the automated processes that flag and block fake or fraudulent reviews prior to publication, and the post-publication review and escalation procedures.

When the App Store is alerted to a concern about a rating or review, it investigates and may remove a review or developer response, and / or disable the ability to review from a user account. In certain cases, ratings and reviews are escalated for further investigation, for example in cases where a reported concern contains malicious activity that infers bodily harm, or child safety and / or child exploitation concerns. Reviews that contain information concerning a criminal offense involving a threat to life or safety will also be escalated and if necessary reported to law enforcement, in accordance with Article 18 of the DSA.

In 2022, App Store processed over 1 billion ratings and reviews, of which more than 147 million were blocked and removed for failing to meet its moderation standards. In 2023, App Store processed over 1.1 billion ratings and reviews. Close to 152 million were removed.

Review and Controls Associated with Recommender Systems

As explained above, users can discover apps available in the App Store through five tabs: Today, Games, Apps, Arcade, and Search. The apps that are displayed in these tabs appear organically (for example, various categories of "Top" charts) in all tabs except Search; as "recommendations" in the form of algorithmically selected recommendations or editorially curated recommendations in all tabs; as a search result in the Search tab; or as an Apple Search Ad in the Today or Search tabs. App recommendations may also be personalised based on a user's demographic, as well as App Store purchase and download history. Notably, all apps appearing in the App Store, including those which are recommended, have already undergone the rigour of the App Review process and have been approved for publication in the App Store.

[CONFIDENTIAL]

Algorithmically Selected App Recommendations

Apple maintains an app repository that describes various attributes of apps during their lifecycle in the App Store. For example, the app repository includes standard app information and metadata supplied by the developer, such as the name of the app and developer, when the app was released, the app categories, and the app's age rating. It also includes information about the app's popularity, including statistics on app downloads and transactions; aggregate and anonymised user engagement signals, such as browse and search activity; and fraud trust signals. [CONFIDENTIAL]

Whether an app appears in recommendations depends on machine learning algorithms that interpret information from the app repository related to: (i) app quality; (ii) app popularity; (iii) app sensitivities; and (iv) the context of the recommendation.

Not all apps may appear as recommendations. [CONFIDENTIAL] For example, if the App Store becomes aware of violations of the Guidelines, the app may be removed from recommendations until the app becomes compliant. [CONFIDENTIAL]

Editorially Curated App Recommendations

The App Store Editorial team uses apps from the app repository to curate its own unique app recommendations. Factors that App Store editors consider when considering recommendations include: (i) user interface design: the usability, appeal, and overall quality of the app; (ii) user experience: the efficiency and functionality of the app; (iii) innovation: apps that solve a unique problem for customers; (iv) localisations: high quality and relevant; (v) accessibility: well-integrated features; (vi) App Store product page: compelling screenshots, app previews, and descriptions; and (vii) uniqueness.

For games, editors also consider: (i) gameplay and level of engagement; (ii) graphics and performance; (iii) audio; (iv) narrative and story depth; (v) ability to replay; and (vi) gameplay controls.

The Editorial team creates a curated catalogue of apps for each category used in the various tabs (for example, original stories, tips, how-to guides, interviews, App of the Day, a Game of the Day, Now Trending, Collections, Our Favorites, Get Started). For each curated category, the Editorial team determines whether to pin certain categories in designated vertical positions of tabs. They can also choose to personalise categories, as described below. If a story has been personalised, the curated category would surface and order stories that are most relevant based on a user's purchase and download history.

[CONFIDENTIAL] The curation guidelines have been distilled into best practices, which are publicly available to help developers understand what the App Store finds valuable in curation for users.[22]

App Store Search Results function

Within the Search tab, users can use the "search" function to search for games, apps and Stories. This search function is designed to help users find the apps they are looking for as efficiently as possible.

Users can search in one of the 40 languages available on the App Store. When a user starts typing a search word they are presented with a number of suggested terms in a list, before they hit the "search" button to action the search. These suggested terms are selected by algorithm. The dominant factor that determines these suggested terms is based on prior aggregate user search behaviour in the storefront in which the user is searching. This user behaviour is tracked on an anonymised basis and not per individual user. If there are few prior searches similar to what a user has started typing, another algorithm will suggest terms based on app name-matching.

When a user clicks on "search" they are presented with search results. These search results are unique to the App Store storefront associated with the user's account. Search results are determined by an algorithm, which determines results based on a number of factors, including:

a) text relevance (for example using an accurate app title), relevant keywords / metadata, and category of app a user has searched for (for example games);

[22] https://developer.apple.com/app-store/discoverability/

b) signals associated with aggregated user behaviour, including app searches and downloads, number and quality of ratings and reviews and app downloads in the storefront the user is searching in; and

c) date of launch in the App Store.

When an app is new and does not have significant numbers of searches or user signals associated with it, it is automatically boosted by the search results algorithm. Once the app has sufficient exposure in the search function, and the algorithm has collected sufficient signals regarding its popularity / quality, the boost is removed.

In limited circumstances, Apple may manually override results by removing or adding a given app listing from the search results. For example, if a developer adds keywords to their listing attempting to rank in queries for which they are not relevant, Apple can remove their result for that search query.

Apple applies the same search algorithm, applying the same factors, to its own apps as it does to third-party apps.

Search results are not personalised. However, some personalisation of the presentation of the results may occur on-device, for example if a user searches for an app that they have already downloaded to their device. In such instances, the search results may include product information about the already downloaded app in a more condensed form.

Apple Search Ads

Apple Search Ads is a service by which developers can pay for promoted placements of their apps in the App Store.

Within the App Store, Apple Search Ads appear in the Today tab, the Search tab and Search results, and in app product pages users access while browsing. These promoted app placements appear on the App Store itself and are distinct from and unrelated to the third-party advertisements that may be shown within an app, for which the developer, and not Apple, is responsible.

Apple Search Ads only feature apps already available in the App Store in the subject country or region.

With Apple Search Ads, it is made clear to users that they are seeing a promoted app placement (as opposed to an editorial / organic placement) through clear and conspicuous visual cues intended to make a clear distinction between promoted app placement and organic content. All such promoted app placements include a prominent “Ad” mark, and may include border and background shading demarcations. Moreover, the “Ad” mark is interactive; when a user taps on it, they see an “About this Ad” sheet, which explains why they are seeing that particular app and what criteria, if any, were used to display the relevant app campaign. If a user clicks on the promoted app, they are taken to the app product page.

Apple Search Ads determines which apps get promoted placement via a bid auction mechanism: advertisers pay only what they are willing to pay in a competitive auction marketplace, based on their individual preferences, including bids for actions like taps or installs.

All developers who promote their apps using Apple Search Ads must contractually commit that their promoted apps will comply with all applicable laws and regulations.

Apple takes several measures to address risk relating to Apple-delivered promoted app placement on the App Store. For example, in addition to the actions performed by the App Review team to review and approve apps for distribution on the App Store, the Apple Search Ads team additionally reviews promoted app placement for content, imagery, and promotion category classification. Apple Search Ads policies prohibit certain categories of apps from being promoted on the App Store – either altogether, in certain countries or regions, or in certain App Store placements.[23] Moreover, some categories of apps that are not prohibited may still face promotion restrictions as managed by the Apple Search Ads team – for example, submitting proof of specific permits or licences to Apple as a prerequisite to advertising, including the promotion of apps, in certain countries or regions.

Additionally, the Apple Search Ads team routinely monitors account and advertiser actions for signs of potential misconduct and handles complaints relating to Apple Search Ads advertising.

Apple Search Ads is engineered to facilitate promoted app placements in a manner that ensures that the App Store does not know which promotional app has been surfaced to a user, or whether an identifiable user has viewed or clicked on it.

Apple creates "segments" to deliver personalised Apple Search Ads on the App Store. Segments are groups of people who share similar characteristics. Information about a user may be used to determine which segments they are assigned to, and thus, which Apple Search Ads they receive. To protect user privacy, personalised Apple Search Ads are delivered only if more than 5,000 people meet the targeting criteria selected by an advertiser.

Information to assign a user to segments is strictly limited and includes account information (for example, name, address, age, gender), downloads, purchases and subscriptions records on the App Store. When selecting which Apple Search Ad to display from multiple ads for which a user is eligible, Apple may use some of this information, as well as App Store searches and browsing activity, to determine which ad is likely to be most relevant. This information is aggregated across users so that it does not identify any single user.

Pursuant to its obligation under Article 39 of the DSA, Apple has created a public online repository of apps promoted as Apple Search Ads.[24] The repository sets out information about each app presented as an Apple Search Ad to consumers within the EU, including what content was presented where, and when. The repository is designed to contain this information for the period that the Apple Search Ad unit is live, and for one year from the date of its last impression. For content that is restricted due to alleged illegality, a governmental order, or incompatibility with applicable terms and conditions, the repository is designed to record the restriction as well as the grounds for the restriction. The repository is accessible and can be queried through a dedicated website. An API is also available for large volume queries.

Apple Search Ads is built with strong limitations to protect children and minors:

a) For a minor under 18 (or the age of majority in the relevant jurisdiction) who is logged in with their Apple ID, the Personalised Ads setting is automatically set to "off" and cannot be enabled until the user reaches the age of majority. With Personalised Ads

---

23 https://searchads.apple.com/policies/

24 https://adrepository.apple.com/

set to off, Apple cannot use account information (for example, name, address, age, gender), apps downloads, or in-app purchases and subscriptions, for serving Apple Search Apple Search Ads in the App Store.

b) When a user turns 18 (or the relevant age of majority), the App Store app will display a prompt to allow the user to choose whether or not to agree to receive personalised Apple Search Ads on the App Store.

Furthermore, as explained in Section 2 above, each app has an age rating. These age ratings, and the age of the user, determine whether, and if so, which Apple Search Ads will be displayed to users under 18 years of age, subject always to the following limitations:

a) Apple Search Ads are not presented to users under the age of 13;

b) All apps rated 17+ are not presented to users under 18 as Apple Search Ads; and

c) Certain categories of apps, irrespective of age rating, are not presented to users under 18 as Apple Search Ads.

For users over 18, it is the developer's responsibility to configure minimum age targeting to local law requirements.

Personalisation

Personalised Recommendations are not available for minors, managed accounts and accounts that have opted out of personalised recommendations.

For a child account, i.e. registered via Family Sharing and under 13 (or the minimum age of lawful consent in the relevant jurisdiction in application of Article 8 of the GDPR), the Apple ID is not eligible to receive any personalised recommendations in the App Store.

Users can change the Personalised Recommendations setting for their Apple ID going to iOS Settings > [user name], tapping Media & Purchases, tapping View Account, and then toggling Personalised Recommendations on or off. Users can also learn more about which information is used to personalise the recommendations made to them (for example information about purchases, downloads, and other activities in the App Store).

If Personalised Recommendations is turned on, user interactions within the App Store may be used to personalise app recommendations and editorial content. For example, the App Store Today tab will recommend content that may be of interest to the user based on what they have previously searched for, viewed, downloaded, updated, or reviewed in the App Store. Recommendations are also based on user purchase history, including in-app purchases, subscriptions, and payment methods together with account information derived from the user's Apple ID.

In addition, personalised recommendations are based on aggregate information about app launches, installs, and deletions from users who choose to share device analytics with Apple, and aggregate information about app ratings.

If Personalised Recommendations is turned off, a user will not receive personalised recommendations or editorial content. Instead, recommendations from the app repository will display apps without reference to the user's engagement with the App Store.

Mitigating potential third-party abuses

The Trust and Safety Operations team is responsible for "live moderation" of App Store hosted UGC and protecting App Store discovery features, including charts and search, from fraudulent behaviour, including the behaviour of "bots". Inauthentic ratings and reviews from fraudulent or bot accounts can mislead users into downloading an untrustworthy app that attempts to game the system through misrepresentation.

The Trust and Safety Operations team uses a number of automated monitoring tools to identify suspicious accounts, apps and app-related activity. These systems help detect suspicious charts and search manipulation. Trust and Safety Operations can take a range of steps to protect against suspicious charts and search manipulation, which include suppressing an app from search for a limited period. They can also take action against developers who repeatedly manipulate App Store discovery features, up to and including termination of developer accounts.

The Trust and Safety Operations team evaluates the efficacy of the automated signals it receives regarding bot accounts and suspicious activity and drives conversations regarding possible improvements.

App Store and Privacy

App Store & Privacy Notice

When first interacting with the App Store, users are presented with service-specific privacy information, in the form of the App Store & Privacy Notice.[25] This ensures that users have an effective choice and any consent to data use on Apple products is fully informed.

Also presented to users at this time is Apple's Data & Privacy Icon, which links to more detailed on-screen information and more detailed service-specific privacy information regarding the App Store's privacy practices. This provides users with transparent and easily accessible information that details how Apple collects, processes and discloses their personal data.

The App Store uses, inter alia, local, on-device processing to enhance its recommendations and mitigate privacy risks. In addition, using data such as app installs – the App Store can suggest apps and in-app events that are more relevant to users. These recommendation systems are described below.

The App Store & Privacy Notice also explains how users can turn off personalisation features. Personalisation is also described in further detail below.

When a user uses a payment card in the App Store, Apple may obtain information from the financial institution or payment network, and also use it for fraud prevention and verification.

Privacy Nutrition Labels

Product pages in the App Store feature a section that includes summaries prepared by developers of their key privacy practices in a simple, easy-to-read label, which informs the user about the app's privacy practices before downloading it. These labels show how developers are collecting and using user data, such as a user location, browsing history, and contacts.

[25] https://www.apple.com/privacy/labels/

The same applies to Apple's own apps.[26] Privacy nutrition labels are an innovative and easily understandable feature which makes use of clear language and images/icons to explain how data is used.

App Privacy Report

The App Privacy Report, accessible via a user's Settings, records data on device and sensor access, app and website network activity, and the most frequently contacted domains in an encrypted form on user devices.[27] Via this report, users are able to see how often their location, photos, camera, microphone, and contacts have been accessed by apps during the last seven days, and which domains those apps have contacted. Users therefore have full and easy visibility into the ways apps use the privacy permissions a user has granted them, as well as their respective network activity. Together with Privacy Nutrition Labels, this feature provides users with transparent information about how the apps made available on the App Store treat user privacy.

App Tracking Transparency Framework

If a developer wants to track a user across apps and websites or access their device's data for advertising purposes, they must seek the user's permission through the App Tracking Transparency Framework. This applies across all apps available on the App Store. Tracking in this instance refers to linking user or device data collected from an app with user or device data collected from other companies' apps, websites, or offline properties for targeted advertising or advertising measurement purposes. Tracking also refers to sharing user or device data with data brokers.

An app tracking section in Settings lets users easily see which of their apps have been given permission to track, so they can change their preferences and disable apps from asking in the future.

Access Permissions and App Sandbox

Apps may request access to features such as a user's location, contacts, calendars, or photos. The App Sandbox protects user data by limiting access to resources requested through entitlements. Users receive a prompt with an explanation the first time an app wants to use this data, allowing them to make an informed decision about granting permission. Developers are required to get permission from users, with a simple, clearly understandable, and prominently placed means before tracking them or tracking their devices across apps and websites owned by other companies for ad targeting, for ad measurement purposes, or to share data with data brokers. Even if a user grants access once, they can change their preferences in Settings at any time. In addition, no app can access the microphone or camera without the user's permission. When an app uses the microphone or camera, the user's device displays an indicator to let the user know it is being used – whether the user is in the app, in another app, or on the Home Screen. In addition, the Control Center on a user's device shows the user if an app has recently used the microphone or camera.

---

26 https://support.apple.com/en-us/HT212958

27 https://www.apple.com/newsroom/2023/05/app-store-stopped-more-than-2-billion-in-fraudulent-transactions-in-2022/

The App Sandbox provides protection to system resources and user data by limiting a developer's app's access to resources requested through entitlements. This creates secure silos to protect the data of end users across the device.

Child Safety and Parental Controls

Child safety

Apple knows that keeping children safe online is imperative and for that reason has created a number of features to help protect children and provide information to parents and guardians to improve children's safety online. These include:

(a) Child Account Creation;

(b) Family Sharing;

(c) Screen Time; and

(d) Ask to Buy.

Child Account Creation. "Family Sharing" is an operating system-level feature that is accessible in the Apple ID section of settings. Using Family Sharing, a family organiser can invite up to five other family members to join the family group and designate an adult family member as a parent/guardian. A parent/guardian, as well as the organizer who can also act as a parent/guardian, can create an Apple ID for users under 13 and enable a range of parental controls to manage their child's experience during the account creation process.[28] The organizer can also enable parental controls when they invite a child between 13-17 to join the family group by selecting Invite in Person in family settings. Child users cannot create an Apple ID themselves if they indicate that they are under 13 years of age; all such accounts must be set up by a parent/guardian or the organizer via Family Sharing.

Family Sharing enables the safe use of Apple devices and products by families and children and allows parents to share access to Apple services. However, there may be times when parents want to limit the child's access to certain types of content or purchases available to the rest of the Family. As noted above, if a user is below the relevant age then a parent must create the Apple ID for the child.

On supported platforms, Screen Time parental controls allow parents to set limits on their child's device and lock changes using a passcode. Screen Time's App & Website Activity features help parents better understand and make choices about how much time their children spend using apps and websites. For example, App Limits can be used to set daily time limits for certain categories of apps, such as social apps and gaming apps. Screen Time reports provide a detailed overview of how much time is spent using apps, visiting websites, and on the device overall, and which apps send the most notifications, which helps parents monitor their child's device use. Downtime lets parents block apps and notifications from launching on Screen Time enabled devices for specific time periods. If downtime is scheduled, parents can use Always Allowed to make exceptions for specific apps, like educational or mindfulness apps.

[28] The specific age thresholds referenced below may be different for a user depending on which country or region is associated with their Apple ID. For more information on the age thresholds, visit https://support.apple.com/en-us/102617.

Parents can use Screen Time's Content & Privacy Restrictions feature to restrict the download of certain types of content, such as apps with specific age ratings, explicit music and podcasts, and movies and TV shows with specific ratings. This feature can also be used to fully restrict the downloading of apps via the App Store, and automatically filter website content to limit access to adult content in Safari and other apps on iOS and iPadOS. Further, through Screen Time, parents can remove apps such as FaceTime and Camera from their child's device Home Screen and place restrictions on certain privacy settings, such as Location Services and Photos, so that their children cannot change those settings themselves without entering the Screen Time passcode.

Screen Time's Communication Limits feature allows parents to choose who their children are communicating with and when throughout the day, including during downtime, so children can always be reachable, whilst providing the knowledge and control to help keep them safe.

Ask to Buy allows parents to approve app downloads and purchases requested by the child, including in-app purchases, on the App Store and content such as a TV show, movie, or book from Apple Media Services. It is enabled by default for any children under 13 and can be enabled for any family member under 18 by the Family Organiser or another parent/guardian in the family group.[29]

If a child initiates a download or purchase on their device, parents receive a request to approve it on their own device. If they chose to approve it, the download or purchase will be added to the child's account. If they decline, the process stops there (i.e. App Store will not complete the download or purchase).

Child Safety

Apple employs dedicated Child Safety Counsel. Child Safety Counsel works with other areas of the Apple business (including those specific to the App Store) relevant to child safety and contribute to policies and procedures to keep children safe when they engage with Apple products and services. Child Safety Counsel is also responsible for investigating escalations from within Apple and third parties (including developers and users) relating to CSAM or CSEA material, and, where necessary, reporting issues to law enforcement agencies.

App Store External Notice and Action Measures

As detailed above, there are multiple proactive controls in the App Store designed to stop problematic apps being published on the App Store. There are further controls in place that ensure that only a smaller subset of apps are recommended to users, either as recommended or editorial content, or as Apple Search Ads.

In addition, there are also various reactive controls in place, which are designed to ensure that users, developers, government agencies and others can alert the App Store to problematic apps that have already been published on the App Store.

Report a Problem

[29] https://support.apple.com/en-us/HT201089

Customers may use the "Report a Problem" feature to submit notices of offensive, illegal, or abusive content concerning apps they have purchased or downloaded. The Report a Problem function is a tool to help users raise concerns to the App Review team and other teams about content they may encounter on the App Store. Consumer protection is a priority of the App Store, and an area of focus for the App Store Trust and Safety Operations team. "Report a Problem" is a cross-functional effort which originated from collaboration between Trust and Safety Operations team engineers and product managers, and their counterparts in the App Review team, and World Wide Developer Relations, to create user- and developer-facing solutions to address common concerns in the App Store.

The Report a Problem link is displayed in the quick links at the bottom of the Games and Apps tabs, or from the product page of any app a user has purchased or downloaded. Users can choose from "report a scam or fraud" and "report offensive, abusive, or illegal content" options to submit their concern about content they have purchased or downloaded. Users are presented with a free text field to describe the issue they are reporting.

[CONFIDENTIAL]

As detailed below, developers have recourse to various appeal mechanisms in the event that they disagree with Apple's decision to remove apps or terminate developer accounts.

Report a Concern

The Report a Concern tool is another key control which allows users and developers to raise concerns regarding the content of specific user reviews, and developer responses to such reviews. Concerns can be raised in relation to any content where reviews are available.

Report a Concern is available to developers in App Store Connect, as well as to developers and users on the App Ratings and Review page, where users can press and hold on the review and Report a Concern will appear in the pop-up menu. The Trust and Safety Operations team works with AppleCare to review external escalations raised via "Report a Concern".

Report a Concern could be used in the following scenarios:

a) Users or developers seeking to flag misleading, offensive, illegal or irrelevant content, or content that otherwise violates the Submission Guidelines of the AMS Terms in reviews. All such flagged reviews are subject to moderation.

b) Where a developer may have posted offensive, illegal, or misleading responses to critical reviews.

c) Developers are encouraged in the event they see a review that contains offensive material, spam, or other content that violates the AMS Terms and Conditions, to use the Report a Concern option under the review in App Store Connect instead of responding to the review.

AppleCare reviews Report a Concern escalations, and performs an initial triage for offensive content, including illegal content, instances of profanity, solicitation, or spam. Reported concerns go into a queue for the AppleCare team, which is trained by Trust and Safety Operations on identifying user review violations, and actioning concerns, as well as escalating issues to other relevant teams as necessary. The AppleCare team receives guidance and training on how to consider a reported concern, including investigation, follow-up and escalation paths.

Following its consideration, AppleCare can leave the review as-is, remove a review or developer response, and / or disable the ability to review from a user account. If a reported concern contains or a threat or reference to suicide, malicious activity that infers bodily harm, child safety and / or child exploitation concerns, or otherwise indicates a safety issue, the AppleCare team is instructed to send an email to escalate the matter directly to Trust and Safety Operations. The Trust and Safety Operations team will then forward the review and its associated data, including reviewer ID and email address, to Apple's Global Security Investigations team for further action, which may include alerting law enforcement. Apple has updated its processes to reflect the requirements in Article 18 of the DSA.

AppleCare continuously monitors new trends among the customer concerns being reported and escalated. AppleCare partners with a variety of teams, including Trust & Safety Operations, to adapt ratings and reviews detection and response measures where appropriate.

Notices Routed to App Store Legal

The App Store Legal team is responsible for reviewing and vetting notices from external sources that involve issues with apps in the App Store. As noted above, Government regulatory authorities send notices to the App Store, including requests for information about an app or developer, or demand to take down an app pursuant to local law or court order, via a dedicated email inbox. Likewise, local law enforcement authorities send notices and requests for information to a similar dedicated email inbox as explained above. In addition, customers, developers, government authorities or other parties may provide notices to various functions throughout Apple, which are then routed to the App Store Legal team.

The App Store Legal team works with the App Review team, which reviews and investigates the app for any issues identified in the government notice. If the App Review team identifies a Guideline violation, they will employ standard operating procedures to engage the developer and ensure the app is brought into compliance with the Guidelines, or remove the app and / or terminate the developer, if the circumstances warrant it. If there is a valid legal basis or government order to remove the app, the App Review team will take appropriate action and may communicate the issue to the developer, as appropriate. This may include removing the app from the local storefront in question, to comply with local law.

Content disputes

Rights holders can submit App Store content disputes via a dedicated webpage.[30] These submissions are routed to the AMS Content Disputes Legal team for consideration.

Once the AMS Content Disputes Legal team receives a complete complaint, the team responds with a reference number.[31] They put the complainant in direct contact with the provider of the disputed app. If needed, complainants can then correspond with the AMS Content Disputes Legal team directly via email. The parties to the dispute are primarily responsible for its resolution.

However, in certain cases, including where the parties are unable to resolve the dispute bilaterally, the AMS Content Disputes Legal team will intervene. The team does not take apps down solely on the basis of fraudulent or anti-competitive claims, but instead will consider a number of factors when deciding whether or not to remove potentially violative apps from the App Store. These include:

a) whether the app or developer has been the subject of other complaints;

b) the frequency of such complaints; and

c) whether there is reasonable indication that an intellectual property violation has occurred.

---

30 https://www.apple.com/legal/intellectual-property/dispute-forms/app-store/

31 In the event that a party abandons a claim, Apple has automated templates which are sent out as reminders, and if no response is received, the matter will be recorded as having been closed.

If there are continued violations by a developer or the developer makes fraudulent misrepresentations of material facts, the AMS Content Disputes Legal team may have a developer's account terminated.

The AMS Content Disputes Legal team addresses and mitigates risks of potential intellectual property violations on the App Store, and prevents repeat offenders from accessing Apple's services and causing subsequent infringements. The AMS Content Disputes Legal team has implemented various controls and processes in order to do so.

Dedicated contact points for government authorities and agencies

Government authorities from law enforcement and various regulatory agencies may send notices requesting information or app removals based on alleged or suspected violations of local law. Authorities send requests to the App Store to takedown or investigate apps via email notice to dedicated email addresses, [CONFIDENTIAL] or, for law enforcement inquiries and notices, lawenforcement@apple.com. These requests are vetted by the App Store Legal team.

Where credible information is received from any source (for example users, developers or law enforcement) that a developer is not acting in accordance with the Guidelines or local law, Apple will investigate and take appropriate action, which may include removal of the app from the App Store and removal of the developer from the Apple Developer Program.

In addition, if Apple is alerted to information on the App Store that gives rise to a suspicion that a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place, as envisaged in Article 18 of the DSA, steps will be taken to notify the appropriate law enforcement authorities.

Content Reports portal for DSA

Apple enhanced its escalation and reporting mechanisms to adequately capture reported concerns relating to Systemic Risks which may stem from the App Store or its use. In that regard, and in connection with its efforts to comply with Article 16(1) of the DSA, Apple enhanced its Report a Problem feature and created a new Content Reports portal, to enable third parties in the EU to report illegal content.

In August 2023, the Report a Problem flow was updated to achieve integration with the new Content Reports portal. If a user on a storefront in the EU engages Report a Problem in the App Store, they can select "Report offensive or abusive content" or "Report illegal content" from the menu of options. If they select the former, the user goes through the process flow outlined above. If they select the latter, they are redirected to the Content Reports portal. The Content Reports Portal can also be accessed directly via the web.

The Content Reports portal is a central platform where individuals, including government representatives, and in due course "Trusted Flaggers", can file notices concerning alleged illegal content, from which communications concerning those notices are processed and sent, and in which data is consolidated for later transparency reporting purposes. Anyone in the EU can submit concerns about alleged illegal content via the Content Reports portal, whether or not they have purchased or downloaded the app in question. Members of the public can in the EU also use the portal to anonymously file notices concerning CSAM content.

[CONFIDENTIAL] All remaining notices will undergo manual triage before submission to App Review. Manual triage will help Apple track and understand the kinds of notices it receives, [CONFIDENTIAL] and help identify possible misuse and abuse of the system. Once a notice passes through these triage systems, an automatic acknowledgment communication will be sent to the notifier.

After undergoing a verification process intended to safeguard the system and prevent abuse, government representatives (and in due course trusted flaggers) can submit notices which bypass the triage systems and are processed on an expedited basis. Government representatives and trusted flaggers will also receive acknowledgment communications when their notice is submitted to App Review for analysis.

The App Review team collaborates with relevant internal teams and partners, including the App Store Legal team when appropriate, to review, analyse, and action the notices. Once an action is taken, the Content Reports portal facilitates necessary communications to notifiers and designated appointees about the actions taken, and when necessary, to impacted consumers who purchased illegal products or services.

If a notifier disagrees with an outcome, they have the option to challenge the decision via https://contentreports.apple.com/Complaints. These complaints are received through a separate section of the Content Reports Portal and are routed to senior App Review analysts for review. The senior App Review analyst reviews the original notice alongside any new information provided by the complainant. These senior App Review analysts partner with relevant internal teams, including the App Store Legal team where necessary, to evaluate the complaints. Some matters may be escalated for review by the ERB. Communications are sent to complainants as part of this process.

In order to meet the DSA transparency reporting obligations, data is collected throughout the various steps in the described content reporting flow.

DSA Compliance function, website and transparency reporting

DSA Compliance function

In order to meet the requirements of the DSA, Apple established a DSA Compliance function, within Apple's Compliance and Business Conduct Department.

The DSA Compliance function is functionally independent from Apple's operational functions. The Head of DSA Compliance reports directly to the ADI Board on matters relating to DSA compliance.

Pursuant to Article 41(2) of the DSA, the Head of DSA Compliance has ultimate responsibility for, inter alia:

a) cooperating with *Comisiún na Meán* and the Commission for the purpose of the DSA;

b) ensuring that all risks referred to in Article 34 of the DSA are identified and properly reported on and that reasonable, proportionate and effective risk-mitigation measures are taken pursuant to Article 35 of the DSA;

c) organising and supervising the activities of the independent audit that ADI will procure in accordance with Article 37 of the DSA;

d) informing and advising relevant Apple management and employees about relevant obligations under the DSA, including planned training on DSA; and

e) monitoring Apple's compliance with its obligations under the DSA.

The Head of DSA Compliance is supported in this role on a day-to-day basis by a number of legal and other functions responsible for work relating to the App Store, including the App Store Legal team, EU Regulatory Legal, and Privacy Compliance.

DSA Information site

Apple has created a DSA information site - https://www.apple.com/legal/dsa/ie, which contains:

a) the contact details of the DSA Head of Compliance, as the DSA Articles 11 and 12 designated point of contact for communications with Member State authorities, the European Commission, the European Board for Digital Services, and developers and users of the App Store;

b) a link to the Content Reports portal;

c) a link to the Ads Repository;

d) a link to the DSA redress page. This lists redress options for anyone who has filed an Article 16 Notice via the Content Reports portal and who wants to challenge Apple's decision, as well redress options for developers and users who want to challenge decisions Apple has taken. The page will be updated in the future as Article 21 out-of-court settlement bodies are established;

e) a link to the average monthly recipients report; and

f) links to the DSA Transparency Reports.

In due course, the Information Site will also include App Store Risk Assessment reports.

DSA Transparency Reports

Pursuant to Articles 15, 24, and 42 of the DSA, Apple publishes App Store DSA Transparency Reports every six months, containing information on orders and notices of illegal content which the App Store has received and content moderation measures which the App Store has taken on its own initiative.