APPLE DISTRIBUTION INTERNATIONAL LIMITED

App Store –
Third 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 2025

App Store – Report on Risk Assessment and Risk Mitigation Measures

This is a non-confidential version of the report on App Store Risk Assessment and Risk Mitigation Measures, prepared by Apple Distribution International Limited ("ADI"), and published in accordance with Article 42(4) of the DSA.

SECTION 1: INTRODUCTION AND BACKGROUND

Section overview

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

2025 report and its structure

The third risk assessment, and this report, covers the period 1 June 2024 to 31 May 2025 (the "**Risk Assessment Period**").

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]

This risk assessment report is structured as follows:

- Section 1 contains an explanation of Apple's approach to its third 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 the design, functionality and features of the App Store.
- Annex 2 (separate enclosure) contains background detail on relevant policies, procedures and controls. This includes information from Apple's February 2025

---

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 2023 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 visionOS App Store. We refer to the "**App Store**" as referring to all of those services.

White Paper on Helping Protect Kids Online,[4] which details the industry-leading tools which Apple is working to provide to parents and developers that help enhance child safety while safeguarding privacy. Annex 2 also includes detail on relevant Apple ecosystem-wide controls.

Ongoing DSA engagement

In addition to its ongoing management of risks of the App Store, since submitting the 2024 App Store risk assessment, Apple has actively participated in the following DSA-related engagements:

1. Met with the European Commission to discuss the 2024 App Store risk assessment and its ongoing DSA compliance efforts;
2. Monitored and considered requests for information issued to other VLOPs and related enforcement activities;
3. Provided the 2024 App Store risk assessment to, and discussed it with, *Coimisiún na Meán*;
4. Engaged in European Commission consultations regarding various aspects of the DSA, including the draft Implementing Regulation laying down templates concerning the transparency reporting obligations of providers of intermediary services and of providers of online platforms;
5. Engaged in the European Commission's consultation in connection with its draft guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of the DSA;
6. Attended the June 2024 DSA Risk Assessment stakeholder event, organised by the Global Network Initiative and Digital Trust and Safety Partnership;
7. Attended the European Commission's May 2025 DSA multi-stakeholder workshop on systemic risks and their mitigation;
8. Engaged with the European Commission on the protection of minors and attended the June 2025 Article 28 workshop in Brussels;
9. Engaged with *Coimisiún na Meán* on the European Commission's draft Delegated Regulation on technical conditions and procedures under which providers of very large online platforms and of very large online search engines are to share data with vetted researchers, and engaged with the European Commission's consultation on this topic; and
10. Engaged with the European Commission and four national competent authorities on the Medical Device Coordination Group's (MDCG) "*Guidance on the safe making available of medical device software (MDSW) apps on online platforms*", including attending two MDCG New Technologies Working Group meetings.

[4] https://developer.apple.com/support/downloads/Helping-Protect-Kids-Online-2025.pdf.

Feedback and additional insights on the conduct of DSA risk assessments from these engagements have been taken into account in conducting this risk assessment.

DSA processes, systems and controls

Apple has in place a number of processes, systems and controls in connection with its DSA obligations. These include the following:

1. Establishment of a dedicated DSA Compliance function. Over the Risk Assessment Period, 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 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 ("**Content Report Portal**")[5] and related systems to track and monitor notices and responses;
3. Establishment of transparency reporting processes. Apple has published five DSA App Store Transparency reports, since the 2023 App Store risk assessment was finalised;[6]
4. Creation of a new DSA Legal webpage,[7] with various data points including points of contact information, a link to the Content Reports Portal, Transparency reports, DSA App Store risk assessments and audit reports, and the Advertising repository;
5. Creation of a new process for DSA researcher data access requests; and
6. Establishment of a process to obtain information from developers who are "traders" in the EU in order to comply with Article 30 of the DSA.

Enhancements to controls

Apple has updated its App Store age ratings, which has resulted in five age rating levels, with three ratings for adolescents: 13+, 16+, and 18+. This allows users a more granular understanding of an app's appropriateness, and developers a more precise way to rate their apps.

Apple's Content Restrictions in Screen Time prevent minors from downloading apps from the App Store that exceed the age ratings their parents set. Furthermore, when children browse apps on the App Store, they will not be shown apps with age ratings higher than the ones set by their parents in Family Sharing in the places where Apple features apps

---

5 https://contentreports.apple.com

6 DSA Transparency reports are available here: https://www.apple.com/legal/dsa/ie/. The latest App Store DSA Transparency report was published in August 2025.

7 https://www.apple.com/legal/dsa/

on our storefronts[8] (like on the Today, Games, and Apps tabs, or in our editorial stories and collections). Apple has also introduced new age rating questions for developers to help identify sensitive content in their app. These new questions cover in-app controls; capabilities; medical or wellness topics; and violent themes in the app or game. The answers will help Apple better calculate a rating for the app. Apple also added the ability for developers to set a higher minimum user age than the rating assigned by Apple. Developers must consider how all app features, including AI assistants and chatbot functionality, impact the frequency of sensitive contact appearing within their app to make sure it receives the appropriate rating.

Apple is also implementing two changes to Apple ID and Family Sharing which will enhance the safety of minors who use the App Store. First, Apple is introducing a new set-up process that will streamline the steps parents need to take to set up a Child Account.[9] Second, parents will be able to easily correct the age that is associated with their child's account if they previously did not set it up correctly. Once they do, parents of children under 13 will be prompted to connect their child's account to their family group (if they are not already connected), the account will be converted to a Child Account, and parents will be able to utilise Apple's parental control options—with Apple's default age-appropriate settings applied as a backstop.

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 Risk Assessment Period. This includes engagement with teams responsible for the following functions:

1. App Review;
2. Recommender Systems;
3. Apple Ads;
4. App Store Editorial;
5. Trust and Safety; and
6. 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, 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

[8] Described in further detail in "Core App Store attributes and functionalities" in Section 2 below.
[9] Before parents set up a Child Account, child appropriate on-device privacy settings will apply.

engagement with, for example, 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 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 the VLOP obligations came into effect. This includes direct engagement with the European Commission and *Coimisiún na Meán,* participation in consultation processes, and active monitoring of issues highlighted in requests for information issued to and enforcement proceedings regarding other VLOPs. This engagement has continued to inform Apple's approach to the assessment of its risk profile and the adequacy of its risk mitigation measures.

Having now concluded its third 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 2023 and 2024 risk assessments remain current and sound. 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.[10] This is intended to inform the ongoing assessment of the Systemic Risks and their risk mitigation measures, which are detailed in Section 3 below.

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. 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 help 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 (as set out in Section 3 below).

App Store content types

As detailed in Annex 1, there are four types of content on the App Store that users can access ((a) apps and related product page information; (b) user ratings and reviews; (c) App Store editorial content; and (d) Apple Ads), and therefore where, in principle, users could be exposed to illegal content and other risks. These content types are described

[10] For the avoidance of doubt, the risk profile of the App Store as described in the 2023 and 2024 App Store risk assessments has not changed. The information in this section is supplemental to the risk profile detail set out in those reports.

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.

In addition, Apple describes 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.

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 2, 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.

Absent any risk mitigation measures, there is an increased risk that 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 2023 and 2024 App Store risk assessments 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 2, 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. 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.

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, and 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,[11] including localised 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

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

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 Ads

Apple Ads are the only type of advertising on the App Store. Apple Ads[12] provide a means for third-party developers to increase the visibility of their apps that are already distributed on the App Store.

Apple 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 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 a separate account (an Apple Ads account), using a different web portal from App Store Connect.

Apple 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 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 Ads is largely the same as for apps, although there is a moderate risk that Apple 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 "personalised" based on, for example, 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

[12] Apple Ads are only available for ad placements on the iOS and iPadOS App Stores.

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; 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 2023 and 2024 App Store risk assessments detail the limits of the App Store risk profile, and the scope of Apple's obligations under the DSA. In particular, they explain 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 communicated to the European Commission previously that user-generated content ("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.[13] 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 of the App Review Guidelines, 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;

[13] 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*".

3. the ability to block abusive users from the service; and
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 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 are not moderated in real time, do not arise on the App Store; and
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.

Apple 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 did not identify any risks in the EU beyond or separate from those listed in Article 34(1) of the DSA that might reasonably be said to stem from the design and function of the App Store, or its use, or to be systemic in nature.

Methodology for 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 3.

For each Systemic Risk, the table contains:

1. **Risk Statement**: Any risk that may stem from the design, functioning or use of an app store without reference to risk mitigation measures, including the extensive risk mitigation measures that were built into the design of the App Store upon its inception;
2. **Inherent Risk**: This records the level of risk without considering the risk mitigation measures in place;
3. **Risk Mitigation Measures**: Measures that are in place on the App Store that mitigate the inherent risk;
4. **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; and
5. **Residual Risk and Observations regarding effectiveness of controls**: This records the level of risk after risk mitigation measures and the performance metrics and other risk indicators have been factored into the assessment. It also records Apple's observations on whether it considers its controls are effective in addressing the relevant risk, taking into account the performance metrics and other risk indicators that Apple has identified as being relevant to any risk. These include (as appropriate) App Review rejections, takedowns and appeals data, Article 9 and 10 orders, Article 16 notices and external commentary and feedback.

Inherent risks and residual risks are categorised 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,[14] where recommendations cannot be personalised).

Controls detailed in Annex 2 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 the App Store's recommender systems have confirmed that, during the Risk Assessment Period, Apple has maintained the applicable existing controls.

(b) Content moderation systems

Apple has in place various content moderation systems on the App Store, which are detailed in Annex 2 and categorised in its DSA Transparency reports. During the Risk Assessment Period, Apple has maintained the content moderation systems detailed in the 2023 and 2024 App Store risk assessments.

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.

Content moderation relating to published ads

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

Content moderation relating to ratings and reviews

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

Apple continues to train and enhance the systems it uses to identify problematic user ratings and reviews. During the Risk Assessment Period, 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 for new types of fraud in user reviews. Moderation tools have also been enhanced to improve efficiency and transparency, including impacted user 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.

(c) 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.

Based on its experience during the Risk Assessment Period, 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 the actions Apple takes against them.

(d) Systems for selecting and presenting advertising

Recital (88) to the DSA provides that "*[t]he advertising systems used by [VLOPs…] can also be a catalyser for the systemic risks*".

As detailed in Section 2 above, the only advertising on the App Store is made possible by using Apple Ads. Use of Apple 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 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 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 Ads terms and conditions.

Apple 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 Ads have confirmed that during the Risk Assessment Period Apple has maintained the controls set out in the 2024 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 with applicable data protection and privacy laws.

This risk assessment, including the assessment of the EU Charter of Fundamental Rights 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 2 and the 2024 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.[15]

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 efforts in 2024 to reduce the occurrence of fraud on the App Store are detailed in Apple's 2024 global fraud prevention analysis.[16] In summary, it states that:

1. In the five years ending 2024, Apple prevented a combined total of over $9 billion in potentially fraudulent transactions, including more than $2 billion in 2024 alone. In 2024, Apple blocked over 4.7 million stolen credit cards and more than 1.6 million accounts from transacting again; and
2. In 2024, Apple**:**
    a. terminated ca. 146,000 developer accounts for potentially fraudulent activity;
    b. blocked ca. 139,000 fraudulent developer accounts from being created;
    c. blocked ca. 711 million potentially fraudulent customer accounts from being created; and
    d. deactivated ca. 129 million fraudulent customer accounts.

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

[16] https://www.apple.com/uk/newsroom/2025/05/the-app-store-prevented-more-than-9-billion-usd-in-fraudulent-transactions/.

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 Risk Assessment Period 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 the App Store uses to monitor Systemic Risks

Apple understands the Commission to consider "performance metrics", to include, without limitation, quantitative performance indicators that help determine objectively whether a given policy, action or measure is successful or not, or that allow the determination of progress towards reaching the objectives of the measure. 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.[17]

(b) Content moderation metrics

This includes measures taken by Apple in the EU in connection with published apps, ratings and reviews and Apple 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 Risk Assessment Period, Apple received one Article 9 order. Apple considers the absence or

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

low number of Article 9 orders and take down notices to be a relevant metric in assessing risks on the App Store.

(d) Article 10 orders

This includes Article 10 and non-DSA information notices. Apple tracks and monitors all such notices. It reports Article 10 orders in its DSA Transparency reports. During the Risk Assessment Period, Apple received 902 orders issued by EU Member States' judicial or administrative authorities to provide information as defined by Article 10 of the DSA.

(e) 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.

(f) External feedback and commentary

This includes, but is not limited to, any feedback that may be received directly from, for example, 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.

(g) DSA Article 21 Requests

If users disagree with a decision that Apple has taken with respect to the App Store to restrict or remove their content or account, or if users disagree with a decision that Apple has made in response to a notice submitted to Apple's DSA Notice and Action portal regarding these services, they are entitled to engage with a DSA certified out-of-court dispute settlement body with a view to resolving the dispute. Apple reports the number of such disputes submitted in its DSA Transparency reports. In the Risk Assessment Period, there were a total of two such disputes.

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.[18]

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
As a general and introductory observation, Apple notes that, save where specifically identified otherwise in the table below, Apple has identified through this risk assessment **no reason to believe** that its risk mitigation measures are anything other than proportionate and effective with respect to mitigating all relevant risks, **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, and remains confident that its risk mitigation measures appropriately, proportionately and effectively address all relevant risks. The observations set out below in the 'Observations regarding effectiveness of controls and residual risk' column should be read subject to this general observation. This risk assessment takes into account, but does not repeat, observations on proportionality and effectiveness from Apple's prior risk assessments.				
Violates Intellectual Property Rights				
App Store being used by developers to distribute apps with the intended functionality and purpose of being copycat apps, and/or to use content, imagery etc. that violates the IP rights of third parties.	**High** – Likelihood potentially high. App stores may be targeted by developers seeking to distribute apps with the intended functionality and purpose of violating IP rights.	• DPLA, including sections 2.8 "Use of Apple Services", 3.3.3 D "Legal and Other Requirements", Schedule 1 section 6.3 "Termination", and sections 2.1(iii), 5.1, 6.2 and 7.3 of Schedule 2. • 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.	• App Review, Rejections, Takedowns and Appeals • Article 9 and 10 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 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.

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

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
		• Dedicated Content Disputes team. Here, and below, this refers to the team referred to in Annex 2. • Notice and action mechanisms. Here, and below, this refers to the various notice and action mechanisms referred to in Annex 2.		
Ratings and reviews being used to engage in IP infringement	**Low** – Ratings and reviews cannot contain video or images, and it is unlikely that ratings and reviews would be used for the purposes of IP infringement.	• DPLA, including sections 2.8 "Use of Apple Services", 3.3.3 D "Legal and Other Requirements", Schedule 1 section 6.3 "Termination". • 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*". • Dedicated Content Disputes team. • Ratings and review moderation. Here, and below, this refers to ratings and review moderation referred to in Annex 2. • Notice and action mechanisms.	• DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 Requests • Content moderation metrics • External commentary and feedback	**Low** - Ratings and reviews can only be submitted by registered users who have downloaded the relevant app, and publication is delayed. There is no chat functionality. 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. 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". 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.
Illegal goods and services related to fraud, scams, and financial offences				
App Store being used to distribute apps with the intended functionality and purpose of facilitating scams and fraud and	**High** – Severity potentially high. App stores may be targeted by developers seeking to	• 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*".	• App Review, Rejections, Takedowns and Appeals • Article 9 and 10 orders, and Article 16 notices	**Low -** Apple employs market leading technology and processes 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

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
engaging in fraudulent payment practices, including bait and switch apps	distribute apps with the intended functionality and purpose of facilitating scams or engaging in fraudulent activities.	• Apple Advertising Terms of Service, including section 6(g)(IX)(B). • App Review procedures. • Ratings and review moderation. • Notice and action mechanisms.	• Content moderation metrics • External commentary and feedback	Account Takeover Detection. The results of Apple's 2024 anti-fraud efforts are detailed in Section 3 above. Apple Ads has comprehensive policies and procedures in place to minimise risk of developers posting prohibited advertising in a given region. However, Apple recognises that the introduction of alternative distribution methods in connection with the EU Digital Markets Act results in the fragmentation of data regarding activity on iOS and iPadOS 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.
Ratings and reviews being used to facilitate scams or fraud	**Medium** – Ratings and reviews do not contain images or video and there is no chat functionality. There is, however, some possible risk of fake ratings and reviews (including via bots) being used to boost engagement	• DPLA, including sections 2.8, 3.2 "Use of the Apple Software and Apple Services", and 3.3.3 D "Legal and Other Requirements". • 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*". • Ratings and review moderation. • Notice and action mechanisms.	• DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 Requests • Content moderation metrics • External commentary and feedback	**Low** - Ratings and reviews can only be submitted by registered users who have downloaded the relevant app, and publication is delayed. 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. 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 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

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
	with apps with intended functionality and purpose of facilitating scams and fraud.			post-publication review and escalation procedures.
Ratings and reviews being used to give a misleading impression regarding apps (including via bots)	**High** – Likelihood potentially high. Ratings and reviews cannot contain images or video and there is no chat functionality. There is, however, some possible risk of fake ratings and reviews (including via bots) being used to boost engagement with apps with intended functionality and purpose of facilitating scams and fraud.	• DPLA, including sections 3.2 "Use of the Apple Software and Apple Services", and 3.3.3 D "Legal and Other Requirements". • 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*", "*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*" or "*plan or engage in any illegal, fraudulent, or manipulative activity*". • Ratings and review moderation. • AppleCare Support. • Notice and action mechanisms	• DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 Requests • Content moderation metrics • External commentary and feedback	**Low** - Ratings and reviews can only be submitted by registered users who have downloaded the relevant app, and publication is delayed. There is no chat functionality. 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. 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 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.

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
Illegal Content, Goods and Services				
App Store being used to distribute apps with the intended functionality and purpose of facilitating dissemination of content, goods or services which are illegal in a particular member state (for example, certain types of real money gambling, animal welfare and non-consensual behaviour (non-consensual image sharing and online bullying)), and self-harm	**Medium** – App stores may be targeted by developers seeking to distribute apps with the intended functionality and purpose of disseminating illegal goods or services.	• 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. • Notice and action mechanisms	• App Review, Rejections, Takedowns and Appeals • DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 Requests • Content moderation metrics • External commentary and feedback	**Low** - Apple maintains comprehensive policies and procedures that mitigate the risk of apps with the intended functionality and purpose of disseminating illegal goods or services via the App Store, including pre- and post-publication controls.

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
Ratings or reviews being used to facilitate or promote illegal content, or illegal goods or services	**Medium** – As above. In addition, ratings and reviews do not contain images or video and there is no chat functionality. Users are not likely to seek from app ratings and reviews any information other than that relating to the app itself. There is, however, some possible risk of fake ratings and reviews (including via bots) being used to boost engagement with apps with intended functionality and purpose of facilitating or promoting	• DPLA, including sections 2.8, 3.2 "Use of the Apple Software and Apple Services", and 3.3.3 D "Legal and Other Requirements". • 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*". • Ratings and review moderation. • Notice and action mechanisms.	• DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 Requests • Content moderation metrics • External commentary and feedback	**Low** - Ratings and reviews can only be submitted by registered users who have downloaded the relevant app, and publication is delayed. There is no chat functionality. 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. 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".

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
	illegal goods or services.			
Violates consumer protection[19]				
App Store product page being used to disseminate apps with the intended functionality and purpose of providing misleading information to consumers, including in relation to the functioning of the app, its content, and payment information.	**Medium** – 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	• 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*", "*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"* or *"plan or engage in any illegal, fraudulent, or manipulative activity"*. • 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.	• App Review, Rejections, Takedowns and Appeals • Article 9 and 10 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 content of this kind that automated screening alone might not detect. Apple-delivered ads using Apple Ads are marked on the App Store. Various complaints mechanisms enable users to complain about apps that do not operate as described.

[19] Privacy law is addressed below at page 39 (right to protection of personal data).

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
	regarding apps, albeit falling far short of the level of risk associated with other platforms, such as with social media platforms where "influencer"-related advertising risks arise.			
Ratings or reviews being used to post content which violates advertising or consumer protection law	**Low** - Ratings and reviews do not contain images or video and there is no chat functionality. Users are not likely to seek from app ratings and reviews any information other than that relating to the app itself. There is, however, some possible	• DPLA, including sections 2.8, and 3.2. • 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 unauthorised advertising, promotional materials, or informational announcements*". • All Apple Ads terms and conditions. • Apple Ads review processes. • Ratings and review moderation. • Notice and action mechanisms.	• DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 Requests • Content moderation metrics • External commentary and feedback	**Low** - Ratings and reviews can only be submitted by registered users who have downloaded the relevant app, and publication is delayed. 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. 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 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

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
	risk of fake ratings and reviews (including via bots) being used to boost engagement with apps with intended functionality and purpose of violating advertising or consumer protection law.			post-publication review and escalation procedures.
Apple Ads being used in a manner that violates advertising or consumer protection law, including by advertising illegal content or misleading content	**Medium** – As above, there is some risk of hidden advertising regarding apps, albeit falling far short of the level of risk associated with other platforms, such as with social media platforms where "influencer" related	• 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 unauthorised advertising, promotional materials, or informational announcements*". • All Apple Ads terms and conditions. • App Review procedures. • Apple Ads review processes. • Notice and action mechanisms.	• App Review, Rejections, Takedowns and Appeals • DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 Requests • Content moderation metrics • External commentary and feedback	**Low** – Apple employs market leading technology and processes 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 2024 anti-fraud efforts are detailed in Section 3 above. Apple Search Ads has comprehensive policies and procedures in place to minimise the risk of developers posting prohibited advertising or otherwise violating consumer protection law in a given region.

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
	advertising risks arise.			
Apple Ads being used to advertise content that is illegal in a particular region	**Medium** – Risk is comparatively lower than on other platforms, as the only advertising in connection with the App Store is through Apple Ads, which only features apps which are already approved through App Review and subject to existing controls.	• DPLA, including sections 2.8, 3.2 "Use of the Apple Software and Apple Services", and 3.3.3 D. • 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*". • All Apple Ads terms and conditions. • App Review procedures. • Apple Ads review processes. • Notice and action mechanisms.	• App Review, Rejections, Takedowns and Appeals • DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 Requests • Content moderation metrics • External commentary and feedback	**Low** - Apple Ads has comprehensive policies and procedures in place to minimise risk of developers posting prohibited advertising in a given region.

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
Child sexual abuse material (CSAM) / Child Sexual Exploitation and Abuse (CSEA)				
App Store being used to disseminate apps with the intended functionality and purpose of containing CSAM/CSEA content / or post such content to app product pages	**High** - The risk profile here is significantly lower than for platforms that enable file sharing / one to one or closed group chat and is therefore limited. Nonetheless, the severity of the consequences for affected persons if such risk were to crystallise is high, and the inherent risk level is therefore high.	• 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. • 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.	• App Review, Rejections, Takedowns and Appeals • Article 9 and 10 orders • Article 16 notices • Content moderation metrics • External commentary and feedback	**Low** - Apple maintains comprehensive policies and procedures to address the limited risk of CSAM / CSEA material being disseminated via the App Store. All Apps are subject to the App Review process, including both automated and human review, which includes the review of product page imagery and app binary. The App Store is not a pornographic or adult platform and pornographic content is prohibited by the App Review Guidelines. There are notice and action mechanisms in place to enable third parties to report allegations of CSAM / CSEA content. Apple maintains dedicated child safety counsel to address allegations of CSAM / CSEA content on the service.
Ratings or reviews being used to share CSAM or CSEA	**Medium** – As above. There is a more limited risk in the context of ratings and reviews, as users have no	• DPLA, including sections 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 "Legal and Other Requirements". • AMS Terms, including Submission Guidelines. • Ratings and review moderation. • Child Safety Counsel / CSAM procedures.	• DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 Requests • Content moderation metrics	**Low** - Ratings and reviews can only be submitted by registered users who have downloaded the relevant app, and publication is delayed. 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

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
	ability to post images or videos, and there is no direct messaging functionality.	• Notice and action mechanisms.	• External commentary and feedback	do not comply with applicable ratings and reviews terms and conditions. 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". Apple maintains comprehensive policies and procedures to address the limited risk of CSAM / CSEA material being disseminated via the App Store. Apple maintains dedicated child safety counsel to address allegations of CSAM / CSEA content on the service.
Incites terrorism or violence				
Developers could distribute apps with the intended functionality and purpose of inciting terrorism or violence, or content in app product pages that incites terrorism or violence	**Medium** - The risk profile here is significantly lower than for platforms that enable file sharing / one to one or closed group chat, and those that facilitate the widespread and rapid dissemination of information. Nonetheless, the severity of the	• 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. • Ratings and review moderation. • Notice and action mechanisms. • Apple Advertising Terms of Service	• App Review, Rejections, Takedowns and Appeals • Article 9 and 10 orders • DSA 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, content moderation, and notice and actions mechanisms. Such content is prohibited by the Guidelines.

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
	consequences for affected persons if such risk were to crystallise is high.			
Ratings and reviews being used to incite terrorism or violence	**Medium** – As above. In addition, ratings and reviews do not contain images or video and there is no chat functionality.	• 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. • AMS Terms, including Submission Guidelines. • App Review procedures. • Ratings and review moderation. • Notice and action mechanisms.	• DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 Requests • 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 content moderation and notice and actions mechanisms. Such content is prohibited by the Guidelines.
Illegal hate speech				
App Store being used to distribute apps with the intended functionality and purpose of promoting illegal or harmful speech, or product page being used to disseminate such speech	**Medium** - The risk profile here is significantly lower than for platforms that that facilitate the widespread and rapid dissemination of information.	• 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.	• App Review, Rejections, Takedowns and Appeals • Article 9 and 10 orders • DSA 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 and ongoing review, including the app binary and app product page information.

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
		• Apple Advertising Terms of Service, including section 6(g). • App Review procedures. • Ratings and review moderation. • Notice and action mechanisms.		
Ratings and reviews being used to post harmful or illegal speech (for example, illegal hate speech, illegal discriminatory content, threats, harassment, or defamatory content)	**Medium** – As above. In addition, ratings and reviews do not contain images or video and there is no chat functionality.	• DPLA, including sections 2.8, 3.2, and 3.3.3 D. • AMS Terms, including Submission Guidelines. • Ratings and review moderation. • Notice and action mechanisms.	• DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 Requests • Content moderation metrics • External commentary and feedback	**Low -** Ratings and reviews can only be submitted by registered users who have downloaded the relevant app, and publication is delayed. 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. 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".

Apple's 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. These terms contribute to Apple's 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.

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

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
As a general and introductory observation, Apple notes that, save where specifically identified otherwise in the table below, Apple has identified through this risk assessment **no reason to believe** that its risk mitigation measures are anything other than proportionate and effective with respect to mitigating all relevant risks, **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, and remains confident that its risk mitigation measures appropriately, proportionately and effectively address all relevant risks. The observations set out below in the 'Observations regarding effectiveness of controls and residual risk' column should be read subject to this general observation. This risk assessment takes into account, but does not repeat, observations on proportionality and effectiveness from Apple's prior risk assessments.				
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 EU Charter				
App Store being used to disseminate 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, or with the intended functionality and purpose of negatively affecting fundamental rights (for e.g. in the cases of CSAM (see above), so-called "revenge	**High** – Severity potentially high. However, 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	• 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 • DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 requests • Content moderation metrics • External commentary and feedback	**Low** - . 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 UGC 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.

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
pornography", "deepfakes", etc.)	and rapid amplification of UGC.			
Ratings or reviews being used to cause negative effects on fundamental rights, including rights to human dignity and respect for private and family life (e.g. in the cases of CSAM (see above), so-called "revenge pornography", "deepfakes", etc.)	**Low** – As above. In addition, ratings and reviews do not contain images or video and there is no chat functionality.	• DPLA, including sections 2.8 "Use of Apple Services", and 3.2 "Use of the Apple Software and Apple Services". • AMS Terms, including Submission Guidelines that state that users must not use the service to "post objectionable, offensive, unlawful, deceptive, inaccurate, or harmful content". • Ratings and review moderation. • Child Safety Counsel / CSAM procedures. • Notice and action mechanisms.	• DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 Requests • Content moderation metrics • External commentary and feedback	**Low** - Ratings and reviews can only be submitted by registered users who have downloaded the relevant app, and publication is delayed. 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. 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".
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 EU Charter				
App Store taking an overly restrictive approach to approving or publishing apps, or making arbitrary decisions regarding content, including ratings and reviews	**Medium** - The risk profile here is significantly lower than for platforms that are used for public discourse and the exchange of ideas, such as news or media service platforms.	• DPLA: All developers are permitted to join the Apple developer program provided that they meet Apple's requirements. • App Review Guidelines, including the Introduction ("*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*"); 1.1 (regarding professional political satirists and humourists). • AMS Terms: Users are permitted to post ratings and reviews of apps they have downloaded, provided that they comply with the Submissions Guidelines.	• App Review, Rejections, Takedowns and Appeals • DSA Article 9 and 10 orders, and Article 16 notices • DSA Article 21 requests • Content moderation metrics • External commentary and feedback	**Low** - 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. For example, 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 2. Requests that are not in accordance with local law would only be actioned if the app otherwise violated the Guidelines.

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
	Apple works with developers to facilitate their launch of compliant, high quality apps, and is not incentivised to take an excessively restrictive approach.	• Apple Ads terms and conditions: Developers are permitted to advertise their apps via Apple Ads, provided that they comply with the applicable terms and conditions. • App Review procedures, including procedures for developers to challenge App Review decisions. • Ratings and review moderation. • Notice and action mechanisms. • Issuing of statements of reason.		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 with respect to negative effects in the EU for media pluralism stemming from the App Store.
The right to non-discrimination under Article 21 of the EU Charter				
App Store discriminating against certain developers when conducting screening, App Review, or responding to notices and actions	**Medium** - 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	• 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. • Ratings and review moderation. • Notice and action mechanisms. • Issuing of statements of reason.	• App Review, Rejections, Takedowns and Appeals • DSA Article 9 and 10 orders, and Article 16 notices • DSA Article 21 requests • Content moderation metrics • External commentary and feedback	**Low** - Apple is not aware of any material 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.

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
	amplification of UGC.			
Actual or foreseeable negative effects on the rights of the child enshrined in Article 24 of the EU Charter (addressing also the risk of negative effects in relation to the protection of minors, under Article 43(1)(d))				
Risk of minors being exposed to content (primarily apps) potentially available on the App Store. Including the risk of minors being 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[20] as identified by the OECD within the App Store, given its limited functionality (limit ed opportunity for exposure to hateful / harmful /	**High** – Severity potentially high given impact on minors. App stores may be targeted by developers seeking to distribute apps with the intended functionality and purpose of exposing minors to illegal/harmful marketing, profiling and financial risks.	• 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. • Notice and action mechanisms. • Screen time and parental controls. • Child Safety Counsel / CSAM procedures. • Personalisation practices and restrictions.	• App Review, Rejections, Takedowns and Appeals • DSA Article 9 and 10 orders, and Article 16 notices • DSA Article 21 requests • Content moderation metrics • External commentary and feedback	**Low** - 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. A 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 App Store is substantially lower than other in-scope

[20] 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).

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
illegal behaviour, and hateful, harmful and illegal encounters).				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. Apple continues to monitor the EU BIK+ strategy, including the ongoing work relating to an EU code of conduct on age-appropriate design, and the work of the Commission's Taskforce on Age Verification. There is a low risk with respect to Conduct Risks and Contact Risks[21] 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).
Actual or foreseeable negative effects on the right of users to privacy, including the right to respect for private life as enshrined in Article 7 of the EU Charter and protection of personal data as enshrined in Article 8 of the EU Charter				
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 lawful basis, and process such	**High** – Potential impact on privacy high. App stores may be targeted by developers seeking to distribute apps with the intended	• 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, Rejections, Takedowns and Appeals • DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 Requests • Content moderation metrics	**Low** - The effectiveness of Apple's risk mitigation measures is ensured firstly by Apple's ongoing compliance with the 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.

[21] 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

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
personal data in a manner that is detrimental to users	functionality and purpose of unlawfully collecting and tracking personal data.	• App Review Guidelines, including introduction 'We also scan each app for malware and other software that may impact user safety, security, and privacy'; 5. 'legal' and 5.1 'privacy'. • AMS Terms, including Submission Guidelines that state that users must not use the service to "*post personal, private or confidential information belonging to others*". • Apple Advertising Terms of Service, and Apple 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.	• External commentary and feedback	
App Store undermining developers' and users' rights to protection of personal data, including by tracking activities over the app store or third-party apps or websites, including for advertising purposes	**High** – Potential impact on privacy is high. App stores may be targeted by developers seeking to distribute apps with the intended functionality and purpose of undermining	• Apple Privacy Policy. • Apple Privacy Governance. • App Store & Privacy Notice.	• DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 Requests • Content moderation metrics • External commentary and feedback	**Low -** The effectiveness of Apple's risk mitigation measures is ensured firstly by Apple's ongoing compliance with the 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.

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
	users' rights to protection of personal data.			
High level of consumer protection, enshrined in Article 38 of the EU 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 2 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

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
As a general and introductory observation, Apple notes that, save where specifically identified otherwise in the table below, Apple has identified through this risk assessment **no reason to believe** that its risk mitigation measures are anything other than proportionate and effective with respect to mitigating all relevant risks, **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, and remains confident that its risk mitigation measures appropriately, proportionately and effectively address all relevant risks. The observations set out below in the 'Observations regarding effectiveness of controls and residual risk' column should be read subject to this general observation. This risk assessment takes into account, but does not repeat, observations on proportionality and effectiveness from Apple's prior risk assessments.				
Actual or foreseeable negative effects on electoral processes				
App store being used to distribute apps with the intended functionality and purpose of interfering with electoral processes	**Low** - The likelihood here is inherently significantly lower than for platforms that facilitate the widespread and rapid dissemination of information.	• 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 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 unauthorised advertising, promotional materials, or informational announcements*". • Apple Ads Terms and Conditions and Advertising Policies, including the 3.15 'prohibition on Political Content'	• App Review, Rejections, Takedowns and Appeals • DSA Article 9 and 10 orders • DSA Article 16 notices • Content moderation metrics • External commentary and feedback • Engagement in EC / Commission stakeholder processes (pre- and post- EU Parliamentary elections) • Points of contact including for government officials and authorities during election periods	**Low** - Bearing in mind its low risk profile in this respect, the App Store risk mitigation measures are reasonable and 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. These conclusions are reinforced by Apple's election interference risk efforts since then. 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.

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
		• 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.		
Ratings and Reviews being used for coordinated campaigns or manipulative behaviour to interfere with electoral processes	**Low** – As above. In addition, ratings and reviews do not contain images or video and there is no chat functionality. Users are not likely to seek from app ratings and reviews any information other than that relating to the app itself.	• 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". • 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 unauthorised advertising, promotional materials, or informational announcements*". • Ratings and review moderation. • Notice and action mechanisms.	• DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 Requests • Content moderation metrics • External commentary and feedback	**Low** - Ratings and reviews can only be submitted by registered users who have downloaded the relevant app, and publication is delayed. 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. 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".
Actual or foreseeable negative effects on civic discourse and public security (including disinformation)				
App store being used to distribute apps with the intended functionality and purpose of	**Low** - The likelihood here is significantly lower than for platforms that enable file	• 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 content. Those	• App Review, Rejections, Takedowns and Appeals • DSA Article 9 and 10 orders	**Low** - The risk mitigation measures Apple has in place provide it with ample basis to take action against threats to public security or civic discourse which may arise in connection with the App Store.

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
undermining public security, e.g. by disseminating extremist content	sharing / one to one or closed group chat, and those that facilitate the widespread and rapid dissemination of information.	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 unauthorised advertising, promotional materials, or informational announcements*". • App Review procedures. • Notice and action mechanisms. • Ratings and review moderation.	• DSA Article 16 notices • Content moderation metrics • External commentary and feedback	
Reviews and ratings being used to undermine public security	**Low** – As above. In addition, likelihood is even lower because ratings and reviews cannot contain AI-generated or other images or videos and cannot be rapidly or widely disseminated on the App Store. Disinformation is a low risk in	• 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 unauthorised advertising, promotional materials, or informational announcements*". • Ratings and review moderation. • Notice and action mechanisms.	• DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 Requests • Content moderation metrics • External commentary and feedback	**Low** - Ratings and reviews can only be submitted by registered users who have downloaded the relevant app, and publication is delayed. 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. 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".

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
	ratings and reviews, as users are not likely to seek from app ratings and reviews any information other than that relating to the app itself.			

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

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
As a general and introductory observation, Apple notes that, save where specifically identified otherwise in the table below, Apple has identified through this risk assessment **no reason to believe** that its risk mitigation measures are anything other than proportionate and effective with respect to mitigating all relevant risks, **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, and remains confident that its risk mitigation measures appropriately, proportionately and effectively address all relevant risks. The observations set out below in the 'Observations regarding effectiveness of controls and residual risk' column should be read subject to this general observation. This risk assessment takes into account, but does not repeat, observations on proportionality and effectiveness from Apple's prior risk assessments.				
Actual or foreseeable negative effects on gender-based violence				
App Store being used to distribute apps with the intended functionality and purpose of promoting or encouraging gender-based violence	**High** – Potential severity is high. That said, the likelihood is significantly lower than for platforms that enable file sharing / one to one or closed group chat, and those that facilitate the widespread and rapid dissemination of information. Nonetheless,	• 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 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 • DSA Article 9 and 10 orders • DSA Article 16 notices • Content moderation metrics • External commentary and feedback	**Low** - Apple's 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.

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
	the severity of the consequences for affected persons if such risk were to crystallise is high.			
Ratings and reviews being used to promote or encourage gender-based violence	**Medium** – There is no ability for users to share images or videos in ratings and reviews and no chat functionality. The App Store is not a pornographic or adult platform.	• 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". • 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*". • Ratings and review moderation. • Notice and action mechanisms.	• DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 Requests • Content moderation metrics • External commentary and feedback	**Low** - Ratings and reviews can only be submitted by registered users who have downloaded the relevant app, and publication is delayed. 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. 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".
Actual or foreseeable negative effects on public health and minors, serious negative consequences to a person's physical and mental well-being				

App Store being used to distribute apps with the intended functionality or purpose of producing negative consequences for a person's physical and mental	**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	*Medical device software apps*
		• DPLA, including Guideline 5.0 "Legal" and section 3.3.3 D "Legal and Other Requirements"
		• App Review Guidelines, including 1.4 that requires medical apps to:
		  • "*clearly disclose data and methodology to support accuracy claims relating to health measurements*" (1.4.1);
		  • "*remind users to check with a doctor in addition to using the app and before making medical decisions*" (1.4.1); and
			• App Review, Rejections, Takedowns and Appeals
			• DSA Article 9 and 10 orders
			• DSA Article 16 notices
			• DSA Article 21 Requests
			• Content moderation metrics
				Low:
				Medical device software apps
				Medical device software apps receive an enhanced review upon submission. App Review also flags apps that may have diagnostic or therapeutic purposes. Developers of these apps will be asked if their app is a medical device if not already declared. If the developer declares the app is a medical device, App Review will request regulatory authorisation documentation. A preliminary review of this

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
wellbeing or on public health	with other online platforms with business models focusing on widespread dissemination and rapid amplification of UGC.	• Submit the link to any regulatory clearances received. • AMS Terms, including the Submissions Guidelines that state that users must not use the service to "*post […] unlawful, deceptive, inaccurate, or harmful content*". • App Review procedures. • Apple Ads Terms and Conditions. • Ratings and review moderation. • Notice and action mechanisms. *Other* • DPLA, including sections 2.8, 3.2, and 3.3.3 D. • App Review Guidelines, including 1.4.2 which specifically addresses "drug dosage calculators"; 1.4.3 which specifically addresses apps that "*encourage consumption of tobacco and vape products, illegal drugs or excessive amounts of alcohol*"; 1.4.5 which 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 Ads terms and conditions. • App Review procedures. • Notice and action mechanisms. • Screen Time and other parental controls.	• External commentary and feedback	documentation is conducted for inconsistencies and to ensure the authorisations relate to the territories where the app will be distributed. It is ultimately the developer's responsibility to comply with relevant legal requirements, as stated in Guideline 5.0 and section 3.3.3(D) of the DPLA. *Other* Apple's risk mitigation measures 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.
Ratings or reviews producing negative effects on public health and physical	**Medium** – Ratings and reviews do not contain images or	• DPLA, including sections 2.8, 3.2, and 3.3.3 D. • 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*".	• DSA Article 9 and 10 orders • DSA Article 16 notices • DSA Article 21 Requests	**Low** - Ratings and reviews can only be submitted by registered users who have downloaded the relevant app, and publication is delayed.

Risk Statement	Inherent Risk	Mitigation Measures	Performance Metrics and other risk indicators	Observations regarding effectiveness of controls and residual risk
and mental well-being	video and there is no chat functionality. Users are not likely to seek from app ratings and reviews any information other than that relating to the app itself. There is, however, some possible risk of fake ratings and reviews (including via bots) being used to boost engagement with apps with intended functionality and purpose of negatively affecting public health and wellbeing.	• Ratings and review moderation. • Screen Time and other parental controls. • Notice and action mechanisms.	• Content moderation metrics • External commentary and feedback	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. 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".
Risks to minors in connection with children's rights are addressed above.				

Annex 1 – App Store Design, Functionality and Features

This Annex provides an overview of the design, functionality and features of the App Store, including how users discover apps.

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.

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 the storefront associated with their Apple ID (their "Home Country" storefront). 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 Home Country storefront and language settings. Editorially curated content (described below) may vary, depending on a user's Home Country storefront.

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.

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".

Games App

In 2025, Apple will launch a new Apple Games App, which will allow players to see all the games users have downloaded from the App Store and allows users to have all their Game Centre friends and groups they have played with in one place, to enjoy their games together. Users can see their shared gaming history, compare achievements, and send friends invite links and party codes using any messaging match. It facilitates player-to-player challenges with other users who are in a user's contacts. Users can explore personalised recommendations based on games that they and their friends are playing and games supporting Game Centre features, that can be played together. The Games App only interacts with gaming apps that have been subject to App Review and therefore does not introduce new risks to users of the App Store.

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; data handling practices; and an age rating.

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 will soon begin collecting regulatory information for medical device apps that will display on the product page. From December 2025, Apple will ask all apps in the (i) Medical and (ii) Health and Fitness categories who seek to distribute on any EU storefront to declare whether or not their app is a medical device. Apps that are declared to be medical devices will need to provide the following information:

1. contact information (email, phone, address);
2. their Single Registration Number in the EU;
3. the device's intended purpose/use statement;
4. safety information for the device (warnings, precautions, etc.); and
5. a link to the device's Instructions for Use on the developer's website.

This information will be displayed on the app's product page. Apps that fit these criteria will have one year to complete this information after which they will be blocked from submitting updates for these apps. New apps that fit these criteria will be required to fill in this information to come onto the store after the one-year deadline. App Review will also have discretion to route through this process apps that appear to be medical devices but do not fall under either category.

Age ratings

Age ratings provide information about age-appropriateness of apps, and parents can limit app downloads that exceed age ratings they have set.

When a developer submits an app to us for distribution, they confirm the types of sensitive content within the app and how frequently it appears, and if the app has certain features that impact what kind of content will be presented. Developers must also answer certain questions, as detailed in the Risk Assessment Report. Apple automatically generates an appropriate age rating for their app, based on the answers provided by developers, indicating the suggested minimum age appropriate to use the app. Developers can also opt-in to choosing the highest rating if they believe it is appropriate for their app.

Apple publishes these age ratings on the App Store page for each app, and Apple rejects apps from the App Store if it discovers that they are misleading or inaccurate. These age ratings are integrated into our operating systems, and work with parental control features like Screen Time and Ask to Buy.

Previously, the global age ratings had four thresholds, including two that covered adolescents, 12+ and 17+. Many users and developers wanted more granularity to reflect the wide range of needs and maturity among this age group. In response to user and developer feedback, Apple updated the age rating thresholds to have five categories of age ratings, with three ratings for adolescent children: 13+, 16+, and 18+ (along with ratings for 4+ and 9+). This allows users a more granular understanding of an app's appropriateness, and developers a more precise way to age rate their apps.

Apple has also provided parents with a new way to provide developers with information about the age range of their children – enabling parents to help developers deliver an age-appropriate experience in their apps while protecting privacy.

Through this new feature, parents can allow their children to share the age range associated with their Child Accounts with app developers. If they do, developers can utilize a Declared Age Range API to request this information, which can serve as an additional resource to provide age-appropriate content for their users. The feature is designed around privacy and users will be in control of their data. The age range will be shared with developers if, and only if, parents decide to allow this information to be shared, and they can also disable sharing if they change their mind. It also won't provide children's actual birthdates. Today, Apple's Content Restrictions in Screen Time prevent children from downloading apps from the App Store that exceed the age ratings their parents set. But we're going to go even further—later this year, when children browse apps on the App Store, they also won't be shown apps with age ratings higher than the ones set by their parents in the places where Apple features apps on our storefront (like on the Today, Games, and Apps tabs, or in our editorial stories and collections).

Additionally, through Media Ratings, Developers can incorporate parents' limits on movie or TV ratings into their apps.

Made for Kids provides parents with a section of the App Store with age-appropriate apps held to even higher standards for privacy and safety.

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

Developers may also engage in paid promotion of their apps in the App Store through Apple 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 Ads, apps may be displayed in the Today tab; the Search tab and Search Results; and in the product page while browsing.

Apple 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 Ads and what criteria, if any, were used to display the app campaign.

Apple Ads is a purely optional service for developers, accessible through an independent account (an Apple Ads account), using a different web portal from App Store Connect. Apple Ads were made available to users in certain EU storefronts five years ago; more were added thereafter. Today, Apple Ads are available to users in most EU storefronts, though only a small percentage of App Store developers choose to promote their apps using Apple Ads. If developers choose to not use the Apple 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 Ads for securing promoted placements. The two services and placement algorithms work separately from each other.

Annex 2 – Overview of policies, procedures, and controls

This Annex provides an overview of the features, policies, and controls that apply through the lifecycle of an app in the App Store – from developer onboarding, through to App Review, and controls available to users to personalise how they interact with the App Store.

Developer Screening, Terms & Conditions

Apple conducts identity verification and screening for all developers who wish to join the Apple Developer Program and before an app can be published.

Developer Screening	
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.
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 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.

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-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 App Review Practices

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. A complete set of metadata must be provided (i.e. if a submission includes "placeholder" text, it will be rejected).

Every app or app update submission approved for submission to the App Store is reviewed by the App Review team, first via automated means and then by human app reviewers.

General App Review Practices	
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 for 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 GDPR.
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 or otherwise signal threats and signals (for example, the presence of malicious URLs or executable code) and provide

	relevant app information to the human review component. The automated review process also conducts checks including [CONFIDENTIAL][22], 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 and other 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 identifying 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, for example, 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 can flag 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 and human review 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. On average, the App Review team reviews nearly 150,000 app submissions each week. In 2024, App Review reviewed 7,771,599 submissions (including app updates); again, almost 25% were rejected. App 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 approved for submission to the App Store undergoes human review. During human review, app reviewers analyse the signals provided by automated systems and review the features and functionality of apps to check 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 and 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 is approved for publication in the App Store. Some manual and automated tagging is applied during the App Review process (i.e. before an app is approved for publication on the App Store), to assist human reviewers to decide whether to approve or reject an app submission, or whether to remove an app from the App Store. 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

[22] https://developer.apple.com/help/app-store-connect/create-an-app-record/add-a-new-app

	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, or any other Guideline violation, 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 can adjust 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.
App Review Escalations and new and emerging issues	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, such as [CONFIDENTIAL], or new technologies [CONFIDENTIAL].

App Review Board (ARB)	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**").[23]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.
Executive Review Board (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.

Post-Publication Reviews / Ongoing Monitoring

Ongoing Monitoring	
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 2024, Apple blocked or removed 17,000 apps for bait-and-switch tactics. 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 Apple to 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. The App Store has a number of automated tools in place to detect malicious behaviour 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

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

	available on the App Store change or add new functionality after approval by the App Review team. Once flagged by automation, these apps can be rereviewed by human app reviewers to evaluate whether intervention is needed. Additionally, developers are required to submit updates to their apps through App Connect for App Review. 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.

App Store UGC 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 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. In 2024, App Store processed over 1.2 billion ratings and reviews. More than 143 million fraudulent ratings and reviews were removed.

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.

Mitigating potential third-party abuses	
Automated Monitoring	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.

Reviews and controls associated with Recommender Systems

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 Ads 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]

Recommender Systems & Search	
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.
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); 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 Ads

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

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

Apple 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.

Apple Ads	
'Ad' Mark	With Apple 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 Ads Terms and Conditions	All developers who promote their apps using Apple Ads must contractually commit that their promoted apps will comply with all applicable laws and regulations.

Apple Ads Reviews	In addition to the actions performed by the App Review team to review and approve apps for distribution on the App Store, the Apple Ads team reviews promoted app placement for content, imagery, and promotion category classification.
Apple Ads Policies & Restrictions	Apple 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. Moreover, some categories of apps that are not prohibited may still face promotion restrictions as managed by the Apple 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.
Apple Ads Monitoring	The Apple Ads team routinely monitors account and advertiser actions for signs of potential misconduct and handles complaints relating to Apple Ads advertising.
Apple Ads Privacy	Apple 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 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 Ads they receive. To protect user privacy, personalised Apple 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, address, age, gender), downloads, purchases and subscriptions records on the App Store. When selecting which Apple Ads 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.
Ad Repository	Pursuant to its obligation under Article 39 of the DSA, Apple has created a public online repository of apps promoted as Apple Ads. The repository sets out information about each app presented as an Apple 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 Ads 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 Ads – default personalisation settings for children and minors	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 set to "off", Apple cannot use account information (for example, address, age, gender), apps downloads, or in-app purchases and subscriptions, for serving Apple Ads in the App Store. 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 Ads on the App Store.

Apple Ads – Age Ratings	Each app has an age rating. These age ratings, and the age of the user, determine whether, and if so, which Apple Ads will be displayed to users under 18 years of age, subject always to the following limitations: a) Apple 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 Ads; and c) certain categories of apps, irrespective of age rating, are not presented to users under 18 as Apple Ads. For users over 18, it is the developer's responsibility to configure minimum age targeting to local law requirements.

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.[24] 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. 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. The same applies to Apple's own apps.[25] 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. 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

[24] https://www.apple.com/ie/legal/privacy/data/en/app-store/
[25] https://support.apple.com/en-us/HT212958

	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. 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.

Personalisation

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. 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.

Personalisation

Restrictions on Personalised Recommendations	Personalised Recommendations is 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. Teen accounts can elect to change this setting and turn on personalised recommendations.
Disabling Personalised Recommendations	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).

External Notice & 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 is recommended to users, either as recommended or editorial content, or as Apple 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.

External Notice & Action Measures	
Report a Problem	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]
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. 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. 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. 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 "Trusted Flaggers" as defined under the DSA, 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 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.

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;
d) Ask to Buy;
e) Age Ratings & Content Restrictions and Filters
f) Made for Kids
g) Family Controls Framework
h) Sensitive Content Analysis Framework
i) Media Ratings
j) Age Assurance

In addition, 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. This function acts as a key ecosystem-wide control to mitigate harms for all illegal harms relating to CSEA.

Child Safety and Parental Controls	
Child Account Creation & Family Sharing	"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. 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. To help parents take full advantage of Child Accounts and parental controls, Apple is making two important changes. First, Apple is introducing a new set-up process that will streamline the steps parents need to take to set up a Child Account for a kid in their family. And if parents prefer to wait until later to finish setting up a Child Account, child-appropriate default settings will still be enabled on the device. This way, a child can immediately begin to use their iPhone or iPad safely, and parents can be assured that child safety features will be active in the meantime. This means even more children will end up using devices configured to maximize child safety with parental controls.

	Second, starting later this year, parents will be able to easily correct the age that is associated with their kid's account if they previously did not set it up correctly. Once they do, parents of children under 13 will be prompted to connect their kid's account to their family group (if they're not already connected), the account will be converted to a Child Account, and parents will be able to utilize Apple's parental control options—with Apple's default age-appropriate settings applied as a backstop.
Screen Time	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. 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. ScreenTime Framework lets developers implement Screen Time on their apps.
Ask to Buy	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. 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).
FamilyControls Framework	Currently, to help users make choices about what apps to download, Apple asks developers to provide important information on their App Store product pages—including whether the app contains n-app purchases, and about the app's privacy practices as part of our Privacy Nutrition Labels. To help users make even more educated choices, Apple will highlight whether apps contain user generated content or advertising capabilities that can impact the presence of age-inappropriate content. Developers will also be able to note when their app has its own content controls, like parental controls or requiring proof of age, that let parents limit their children's access to content in the app that might exceed its age rating.

SensitiveContent Analysis Framework	This is a tool provided to developers to allow them to test their app's response to nudity in media, and helps apps check for and blur nudity before it is displayed.
Age Assurance	The Declared Age Range API is a narrowly tailored, data-minimizing, privacy-protecting tool to assist app developers who can benefit from it, allowing everyone to play their appropriate part in this ecosystem. It gives children the ability to share their confirmed age range with developers, but only with the approval of their parents. This protects privacy by keeping parents in control of their children's sensitive personal information, while minimizing the amount of information that is shared with third parties. The limited subset of developers who actually need to collect a government-issued ID or other additional sensitive personal information from users in order to meet their age-verification obligations can still do so, too. All in all, it gives developers a helpful addition to the set of resources that they can choose from—including other third-party tools—to fulfil their responsibility to deliver age-appropriate experiences in their apps.

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; e) a link to the average monthly recipients report; f) links to the DSA Transparency Reports; and g) links to 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.
DSA Risk Assessment Reports	Pursuant to Articles 34 and 35 of the DSA, Apple publishes its DSA Risk Assessment Reports which set out the results of Apple's annual assessment of the systemic risks stemming from the design, function or use of the App Stores in the EU, as well as its assessment of the risk mitigation measures that it has put in place to address those risks.
DSA Audit Reports	Pursuant to Article 37 of the DSA, Apple publishes its DSA Audit Report, setting out the results of the annual independent audit of the App Store's Chapter III DSA obligations.