# APPLE DISTRIBUTION INTERNATIONAL LIMITED

## App Store –

## 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)*

28 August 2023

## App Store – Report on Risk Assessment and Risk Mitigation Measures

## OVERVIEW

This Risk Assessment Report is structured as follows:

Section 1 provides an overview of the Commission's decision to designate the five App Stores as a Very Large Online Platform under the Digital Services Act, an overview of the role of Apple Distribution International Limited, and a summary of the Article 34 and Article 35 DSA obligations.

Section 2 provides an overview of the methodology and steps taken by Apple to carry out the risk assessment, which included discussions with relevant functions within Apple, documentary research and review, controls mapping, the approach to risk assessment and consideration of existing App Store risk mitigation measures, and preservation of documents.

Section 3 provides an overview of relevant Apple ecosystem (i.e. not App Store specific) functions, policies and protections. These apply to the use of all Apple devices, before, or indeed regardless of whether, a user engages with the App Store. This Section details practices and features relevant to user privacy, the protection of minors, Apple's approach to human rights, and its financial crime risk mitigation measures. These features and practices do not form part of the design, function or use of the App Store specifically, but nevertheless form part of Apple's approach to providing safe and trusted products and services to its customers. These practices are therefore described as background and wider context for the assessment of the risk and mitigation measures linked to the App Store's design, function and use. This Section 3 and Section 4 of the Report are included to assist those unfamiliar with key Apple ecosystem policies and practices and the operation of the App Store.

Section 4 provides an overview of the risk profile of the App Store, as the VLOP regulated under the DSA, both from the perspective of an end user, as well as a developer perspective. This Section is intended to provide the reader with a high-level overview of the operation of the App Store and key risk mitigation measures, to assist in understanding the assessment contained in Section 5 as to how the Systemic Risks might stem from the design, function or use of the App Store. As described below, a fuller explanation of the risk mitigation measures deployed in connection with the App Store is set out at Section 6.

Section 5 sets out Apple's assessment of whether and how any of the Article 34 Systemic Risks stem from the design, function or use of the App Store. Consistent with the Commission's expectations, Apple has, to the extent possible, sought to assess how each of the Systemic Risks could arise in principle from the design, function or use of the App Store, without reference to the extensive risk mitigation measures that are in place. This is notwithstanding the fact that, as many of those risk mitigation measures have been in place, and have been continuously enhanced, since the App Store's introduction 15 years ago, they are now deeply integrated in the App Store, rendering the assessment of Systemic Risk without reference to those measures potentially artificial in places.

Section 6 then provides detailed information on the App Store Article 35 risk mitigation measures that are relevant to the Systemic Risks identified in Section 5. This includes a summary of key terms and conditions, including the App Store Review Guidelines, for both developers and users, a detailed description of the App Review process, a summary of key functions involved in escalations of concerns or incidents, a summary of monitoring that continues after apps are published on the App Store, and detailed information on App Store notice and action procedures which enable third parties to alert Apple to concerns regarding content on the App Store as well as problematic content in live apps, and descriptions of relevant recommender systems.

Section 7 concludes with an analysis of the reasonableness, proportionality and effectiveness of Apple's risk mitigation measures, as detailed in Section 6, in managing the Systemic Risks to the extent that they may stem from the design, function or use of the App Store, as identified in Section 5.

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

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

## SECTION 1: VLOP DESIGNATION AND RISK ASSESSMENT AND RISK MITIGATION OBLIGATIONS

### 1.1 Section overview

1.1.1 This Section of the Report provides an overview of the designation of the App Store as a Very Large Online Platform ("VLOP"), an overview of the role of Apple Distribution International Limited, and the Digital Services Act (the "DSA") risk assessment and risk mitigation obligations.

### 1.2 Article 33(4) VLOP designation

1.2.1 On 26 April 2023, pursuant to Commission Decision C(2023) 2726 final of 25 April 2023, the European Commission (the "Commission") notified Apple Distribution International Limited (hereafter, "ADI") that it had designated Apple's "*App Store*" as a VLOP in accordance with Article 33(4) of the DSA. Article 1 of the Decision describes "*App Store*" as "*App Store, consisting of iOS App Store, iPadOS App Store, watchOS App Store, macOS App Store, and tvOS App Store*".[1]

### 1.3 The role of ADI

1.3.1 ADI is a company registered in Ireland and ultimately owned by Apple Inc. ADI is responsible for the provision of the App Store across the European Union ("EU"), and is therefore the "*provider*" of the VLOP service (i.e. the App Store) for the purposes of the DSA.

1.3.2 As such, ADI's board of directors (the "ADI Board") is the "*management body of the provider of the [App Store]*" that is responsible for the "*sound management of systemic risks identified pursuant to Article 34*", as required by Article 41 of the DSA.

1.3.3 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 Risk Assessment, 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.

[1] ADI does not accept that iOS App Store, iPadOS App Store, watchOS App Store, macOS App Store, and tvOS App Store all form part of a single online platform. 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, and tvOS App Store. We refer to the "App Store" as referring to all of those services.

### 1.4 Overview of Articles 34 and 35 obligations on Risk Assessment and Risk Mitigation

1.4.1 Article 34 of the DSA requires each VLOP provider to identify, analyse and assess any "…systemic risks in the [EU] stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services."

1.4.2 The risk assessment must be carried out within four months of the designation (i.e. by 28 August 2023) and at least once every year thereafter, and in any event prior to deploying functionalities that are likely to have a critical impact on the risks identified in Article 34.

1.4.3 The risk assessment must be specific to the VLOP's service and proportionate to the systemic risks, taking into consideration their severity and probability. This recognises that different types of online platforms that have been designated as VLOPs will have different risk profiles.

1.4.4 Pursuant to Article 34, systemic risks within the EU include:

(a) "*dissemination of illegal content;*"

(b) "*any actual or foreseeable negative effects for the exercise of fundamental rights…;*"

(c) "*any actual or foreseeable negative effects on civic discourse, electoral processes, and public security;*" and

(d) "*any 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*",

hereafter referred to as the "Systemic Risks". Section 5 below includes further detail on each of them.

1.4.5 When conducting the Article 34 risk assessment, VLOPs must take particular account of whether and how the following factors influence the Systemic Risks:

(a) "*the design of their recommender systems and any other relevant algorithmic system;*"

(b) "*their content moderation systems;*"

(c) "*the applicable terms and conditions and their enforcement;*"

(d) "*systems for selecting and presenting advertisements;*" and

(e) "*data related practices of the provider*".

1.4.6 In addition, VLOPs must "*analyse whether and how the [Systemic Risks] are influenced by intentional manipulation of their service, including by inauthentic use or automated exploitation of the service, as well as the amplification and potentially rapid and wide dissemination of illegal content and of information that is* *incompatible with their terms and conditions.*" They must also "take into account specific regional or linguistic aspects, including when specific to a Member State."

1.4.7 Further, Article 35 of the DSA requires providers of VLOPs to put in place "*reasonable, proportionate and effective mitigation measures, tailored to the risks*" identified through the risk assessment carried out pursuant to Article 34.

## 1.5 This Report

1.5.1 This Report on Risk Assessment and Risk Mitigation Measures (the "Report" or "Risk Assessment") details the risk assessment conducted by Apple pursuant to Article 34, which includes consideration of existing controls that are already in place to keep the App Store a safe and trusted place for users, as well as any specific mitigation measures identified pursuant to Article 35 to address any Systemic Risks. This Report reflects the position as at the date of finalisation of the report, 28 August 2023.

1.5.2 A schedule detailing teams and functions referred to in the Report is provided at Schedule A.

1.5.3 Pursuant to Article 37 of the DSA, amongst other DSA obligations, Apple's compliance with Articles 34 and 35 will be subject to independent audit. Apple's subsequent risk assessments, including for year 2024 onwards, will factor in any feedback from its auditors, as well as any feedback from or guidance published by the Commission.

## SECTION 2: RISK ASSESSMENT AND RISK MITIGATION METHODOLOGY

### 2.1 Section overview

2.1.1 This Section of the Report details the steps taken by Apple to comply with its obligations under Articles 34 and 35 of the DSA.

### 2.2 Risk Assessment coordination and key responsibilities

2.2.1 This Risk Assessment was coordinated by the App Store Legal team, a dedicated team of inhouse counsel who have primary responsibility for all legal and regulatory issues relevant to the App Store, in collaboration with Apple Privacy Compliance Legal, EU Regulatory Legal, Services Special Programs and other relevant teams and Apple stakeholders.

2.2.2 EU external counsel at Gibson, Dunn & Crutcher LLP was engaged for the purposes of assisting the App Store Legal team in connection with Apple's conduct of the Risk Assessment, including its consideration of the reasonableness, proportionality and effectiveness of the existing App Store mitigation measures which are relevant to the Systemic Risks.

2.2.3 The risk assessment was conducted in parallel with Apple's work to implement new processes and controls to fulfil Apple's obligations under the DSA, including the establishment of a DSA compliance function, reporting to the ADI Board. Where relevant, new controls and processes are factored into Apple's assessment of whether it has in place reasonable, proportionate and effective mitigation measures to address any Systemic Risks stemming from the design, functionality or use of the App Store.

### 2.3 Identification of key relevant stakeholders and controls mapping

2.3.1 In 2022, having identified the App Store as a service likely to be designated as a VLOP pursuant to Article 33(1) and (4) of the DSA, Apple commenced a review of the relevant existing control framework and the extent to which those controls address potential Systemic Risks.

2.3.2 Apple identified key relevant stakeholders that would need to be consulted at the outset of this process, in order to map the relevant processes and workflow carried out by each team, including at different stages of an app's lifecycle. This scoping assessment also considered applicable terms and conditions, enforcement of App Store Review Guidelines (the "Guidelines"), escalation intake and triage mechanisms, moderation of App Store-hosted user-generated content ("UGC"), and other controls, policies, and procedures relevant to the App Store.

2.3.3 The App Store Legal team collaborates with the impacted teams on a routine basis in relation to the management and mitigation of risk within the App Store, and reviews, authors, and updates key App Store policies, including the Guidelines, the Apple Developer Program License Agreement ("DPLA") and related Schedules, as well as App Store-related provisions of the Apple Media Service Terms and Conditions ("AMS Terms"). Based on these prior engagements and initial scoping activities, the App Store Legal team identified relevant teams and senior employees, including those responsible for App Review, Recommender Systems, Global Security Investigations, Privacy Legal and Privacy Compliance, Human Rights, and Trust and Safety Operations, to be consulted in the preparation of this Risk Assessment.

## 2.4 Scoping discussions

2.4.1 Apple conducted a series of scoping discussions with key stakeholders, in order to better understand the key relevant App Store operational processes and procedures and related controls.

2.4.2 The issues addressed in those meetings extended to:

(a) the role of each team in mitigating potential risks relating to the App Store;

(b) the functioning and operation of each team and the ways in which they interact with and rely upon the work of other teams within the App Store;

(c) key stages in the app lifecycle at which Systemic Risks may require mitigation;

(d) the risk mitigation measures in operation to keep the App Store a safe and trusted place for all users, including in relation to illegal content, disinformation and fraud;

(e) the extent to which the design, functionality or use of the App Store could give rise to Systemic Risks;

(f) the operation of any recommender systems, and the use of any algorithmic systems;

(g) the additional risk mitigation measures in operation to further enhance the protection of minors;

(h) internal and external escalation mechanisms and investigation procedures;

(i) the procedures in place within each team to monitor and analyse trends arising from the management and mitigation of risks;

(j) the frequency with which procedures or controls relating to each team are reviewed; and

(k) the effectiveness of relevant risk mitigation measures in addressing key areas of risk for the App Store.

## 2.5 Consideration of external commentary (government, NGO, trade bodies and interest groups, press, developer and consumer) on extent to which the Systemic Risks stem from the design, functionality or use of the App Store

2.5.1 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. This includes commentary from government bodies, NGOs, relevant trade bodies and interest groups, as well as the press. They are also alive to and responsible for considering concerns raised by the extensive App Store developer community and its users. Such concerns and issues have been considered as part of this Risk Assessment.

2.5.2 Discussions were held with Apple functions that interact with external parties, including government agencies and human rights organisations, in order to understand any views raised about the App Store.

## 2.6 Assessment and identification of any Systemic Risks

2.6.1 Apple then assessed the extent to which any potential Systemic Risks stem from the design, functioning or use of the App Store, including by reference to the factors listed in Article 34(2) of the DSA.

## 2.7 Desktop review of documentation of relevant risk mitigation measures

2.7.1 Following the initial scoping discussions referred to above, and with the assistance of personnel within the App Review team, Recommender Systems, Trust and Safety Operations, and other functions, Apple gathered relevant documentation, building upon the understanding of the systems, controls, decision-making, and communication structures within the App Store critical to the management of risks, in particular those relating to the enforcement of the Guidelines through automated and human review of new app and app update submissions, internal escalation/external report intake procedures on app and App Store hosted content, and related supervision, oversight and monitoring. The applicable provisions within the Guidelines, the DPLA and other pertinent documentation are addressed further below.

## 2.8 Consideration of data and documentation relevant to assessment of the effectiveness of existing risk mitigation measures

2.8.1 Documentation relevant to the assessment of the effectiveness of existing controls was gathered and reviewed.

## 2.9 Assessment of reasonableness, proportionality and effectiveness of existing controls in the light of the foregoing

2.9.1 As explained in further detail below, Apple already had in place extensive controls to keep the App Store a safe place for all users. Taking these into account, Apple conducted an assessment of whether those controls, as well as additional controls being implemented in connection with the DSA, constitute reasonable, proportionate and effective risk mitigation measures (factoring in the severity and probability of the Systemic Risks identified earlier in the risk assessment process).

## 2.10 Approach to preservation of documents

2.10.1 Pursuant to Article 34(3), VLOPs must preserve the supporting documents of this Risk Assessment for at least three years.

2.10.2 To comply with this obligation, Apple has retained all documentation obtained from various functions and subsequently reviewed as part of this risk assessment. Apple has also retained as documents "screen grabs" of any relevant information that is currently available online, which may be changed in the normal course of business. All such documentation will be preserved in accordance with Article 34(3) of the DSA.

## SECTION 3: APPLE ECOSYSTEM FUNCTIONS, POLICIES AND PROTECTIONS

### 3.1 Section overview

3.1.1 This Section of the Report details certain relevant Apple-level (i.e. non-App Store specific) functions, policies and practices that apply to all of Apple's products and services across the wider Apple ecosystem.

3.1.2 These protections apply to the use of all Apple devices, regardless of whether a user engages with the App Store, and, while not forming part of the design or function of the App Store itself, and the provision of the App Store by Apple, they contribute to the overall risk environment in which the App Store operates. These protections are not limited to, but extend to, Apple in relation to its provision of the App Store.

### 3.2 Privacy and personal data

3.2.1 Apple recognises that privacy is a fundamental human right. It is also one of Apple's core values.

#### *(a) Privacy by Design*

3.2.2 Apple designs its products and services according to the principle of "*privacy by design*". Apple is widely recognised, including by industry and data protection experts, as setting the industry standard for minimising personal data collection. Apple builds privacy protections into everything it makes, including the devices and operating systems on which the App Store is designed to be used and its related processes, including the comprehensive App Review process, detailed further in Sections 4 and 6 below.

3.2.3 Apple deploys industry-leading user control mechanisms to allow its customers to choose whether to share data such as their Location, Contacts, Microphone, Camera, Health information, and more with apps. In addition, powerful security features help prevent anyone except the individual user from being able to access their own information.

3.2.4 When Apple does collect personal data, Apple retains it for only so long as necessary to fulfil the purposes for which it was collected, including as described in Apple's Privacy Policy[2] or in Apple's service-specific privacy notices, or as long as required by law.

3.2.5 Privacy is a foundational part of the design process. Apple is constantly working on new ways to keep users' personal information safe and protect their privacy. Apple's Privacy Engineering team ensures that privacy protections are incorporated throughout Apple products, apps, and services. Apple's "Feature" page provides an overview of privacy features embedded in its apps and services, including the App Store.[3]

[2] https://www.apple.com/legal/privacy/en-ww/

[3] https://www.apple.com/privacy/features/

3.2.6 Apple believes that users can have great products and great privacy. Five principles are at the core of how Apple achieves this goal:

### (i) Data minimisation

3.2.7 Apple's approach is to collect only the personal data required to deliver what users need. In instances where specific personal information is necessary, Apple minimises the amount of data that it uses to provide the intended service – such as a user's device location when searching in Maps. Apple does not maintain a comprehensive data profile of user activity across all its products and services to serve targeted advertising.

### (ii) On-device intelligence

3.2.8 Apple uses machine learning to enhance user experience – and user privacy – by processing some user data on-device so that third parties, including Apple, do not see and have no access to user data. In those instances in which user data may be sent to Apple or third parties, Apple provides end users with choices, including transparent control mechanisms. Apple has used on-device processing for on-device image and scene recognition in Photos, predictive text in keyboards, and more. Developers can use Apple's frameworks, such as Create ML and Core ML, to create powerful new app experiences that do not require user data to leave their device. That means apps can analyse user sentiment, classify scenes, translate text, recognise handwriting, predict text, tag music, and more without putting privacy at risk.

### (iii) Transparency and control

3.2.9 When Apple does collect personal data, Apple is clear and transparent about it. Apple makes sure users know how their personal data is being used, and, if applicable, how to opt out at any time. Data and privacy information screens help Apple users understand how Apple will use personal data before users sign in or start using the service or any new features. To ensure that Apple is meeting its own high standards for protecting user data and privacy, Apple has conducted a comprehensive review of its services, products and features that collect and/or hold a user's data. This information is available in Apple's "Data & Privacy summaries", which are published on its website.[4]

3.2.10 Apple also provides a set of dedicated privacy management tools on Apple's "Data & Privacy" page.[5] This complete set of self-service tools includes options for users with an Apple ID[6] to: (i) get a copy of the data that they store with Apple that is associated with their Apple ID; (ii) transfer a copy of their data to another participating service; (iii) deactivate their Apple ID temporarily; (iv) delete their Apple ID – and the data

[4] https://www.apple.com/legal/privacy/data/

[5] https://privacy.apple.com/

[6] An Apple ID is the account a customer uses to access all Apple services and to make their devices work together. When creating an Apple ID a user must provide their full name, date of birth, and an email address or phone number. Additional detail for users is available here: https://support.apple.com/apple-id

associated with it – permanently; (v) request a correction to their personal data; and (vi) find out about the types of data that Apple collects.

#### (iv) Protecting user identity

3.2.11 Apple has developed technologies to enable users to obscure their identity when data must be transferred to Apple servers. Sometimes Apple uses random identifiers so a user's data is not associated with their Apple ID. Apple has pioneered the use of "Differential Privacy" to understand patterns of behaviour while protecting an individual user's privacy.[7] By way of example, if a user chooses to send Apple analytics about their device usage, the collected information does not identify them personally. In such cases, to ensure that no personal data is being shared, Apple randomly generates device identifiers that cannot be traced back to a piece of hardware, a customer, nor any identifier in any other data source at Apple. In addition, for particularly sensitive data, Apple applies further de-identification techniques on-device to further reduce any remaining risks of fingerprinting by using techniques such as "Differential Privacy" or by omitting content. Techniques like these help Apple deliver and improve services while protecting users' privacy.

#### (v) Data security

3.2.12 Security is at the core of how Apple has designed its operating systems, products and services. Every Apple device combines hardware, software, and services designed to work together for maximum security and a transparent user experience. Custom hardware – such as the Secure Enclave, a dedicated secure subsystem, in iPhone, iPad, and Mac, which is isolated from the main processor – powers critical security features like data encryption.[8] Software protections work to help keep the operating system and third-party apps safe. Services provide a mechanism for secure and timely software updates; to power a safer app ecosystem, secure communications, and payments; and to provide users a safer experience on the web. Apple devices help protect not only the device and the data stored therein, but the entire ecosystem, including what users do locally, on networks, and with key web services. Apple devices also have encryption features to safeguard user data and enable a remote wipe in the case of device theft or loss.

### *(b) <u>Privacy Governance</u>*

3.2.13 Apple takes a cross-functional approach to privacy governance. Privacy governance covers all areas of the company and covers both customer and employee data. The Vice President in charge of Privacy and Law Enforcement Compliance reports directly to Apple's General Counsel. Apple also has a dedicated Privacy Engineering team that partners with the Privacy Legal team and dedicated product counsel to design products from the ground up, in a way that protects customer privacy and to ensure that Apple protects any data that is within Apple's control. This includes strong

[7] https://www.apple.com/euro/privacy/e/generic/docs/Differential_Privacy_Overview.pdf

[8] https://support.apple.com/en-gb/guide/security/secf020d1074/1/web/1

processes involving Apple's Data Protection Officer, notably around ensuring that data is collected lawfully and is used only for the intended lawful purposes.

3.2.14 Apple also has a Privacy Steering Committee chaired by Apple's General Counsel, with members including Apple's Senior Vice President of Machine Learning and AI Strategy and a cross-functional group of senior representatives.[9] The Privacy Steering Committee sets privacy standards for teams across Apple and acts as an escalation point for addressing privacy compliance issues for decision or further escalation.

3.2.15 Apple regularly engages with a wide range of civil society representatives globally on various privacy and freedom of expression issues, including privacy by design and encryption.

3.2.16 Apple maintains current ISO 27001 and 27018 certifications. ISO 27001 is an international standard for implementing, managing and maintaining information security within a company. ISO 27018 is an international standard for the protection of personally identifiable information in public clouds. To maintain these certifications, Apple is subject to annual audits.

3.2.17 Apple's "Privacy Governance" page provides more details on Apple's approach to privacy governance, including the oversight and monitoring of privacy and data security, the privacy training that all Apple employees are required to take, Apple's data security and incident response, and how Apple handles privacy complaints and private requests for user information.[10]

#### *(c) Privacy Impact Assessments*

3.2.18 As part of Apple's commitment to privacy and other human rights, trained reviewers undertake Privacy Impact Assessments ("PIAs") for Apple's major products and services. PIAs are conducted when Apple is developing new products, services or features. Teams responsible for the development of such products or services must describe in detail how personal data will be processed, and the purposes, retention periods and other processing details. Reviews include assessments of how a product or service processes personal data, the necessity and proportionality of such processing, the risks or impact that any such processing has on individuals and their rights, and the mitigating controls implemented to address such risks or impact. PIAs are approved by Apple's Data Protection Officer.

### 3.3 Advertising and privacy

3.3.1 Apple's Advertising & Privacy service-specific privacy notice describes Apple's data-related practices in relation to its advertising activities and app promotion options, including Apple Search Ads on the App Store (described in Section 4 below).

[9] The Privacy Steering Committee consists of Apple's General Counsel as well as senior representatives from Internet Software and Services, Software Engineering, Product Marketing, Corporate Communications, Information Services & Technology, Information Security, Privacy Legal and the Head of Business Assurance.

[10] https://www.apple.com/legal/privacy/en-ww/governance/

3.3.2 The notice sets out how Apple's advertising platform is designed to protect users' privacy and give them control over how Apple uses their information. The Policy states at the outset that "*[Apple's] advertising platform doesn't share personal data with third parties.*" Apple's advertising platform does not track any user, meaning that it does not link user or device data collected by Apple with user or device data collected from third parties for targeted advertising or advertising measurement purposes, and does not share user or device data with data brokers.

3.3.3 The notice provides detailed information about the minimal data that could be used to personalise Apple Search Ads to users, as well as information about how they can turn ad Personalisation on or off. Further information on ad Personalisation is set out in Section 6 below.

### 3.4 Protections relating to children

#### *(a) Child safety*

3.4.1 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 Set-Up;

(b) Family Sharing;

(c) Screen Time; and

(d) Ask to Buy.

3.4.2 Child Account Set-Up. "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 set up accounts for users under 13 (or relevant age in their country or territory of residence).[11] When setting up an account for a child under 13 (or relevant age in their country or territory of residence), parents and guardians can choose to enable a range of parental controls to manage their child's experience. Child users cannot create an Apple ID themselves if they indicate that they are under 13 years of age (or relevant age in their country or territory of residence); all such accounts must be set up by parents via Family Sharing.

3.4.3 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.

3.4.4 Screen Time provides parents and children an insight into the time the child is spending using apps, visiting websites, and on the device overall, and provides weekly

[11] For residents in the EU, the relevant age is 13 (or the minimum age of lawful consent in the relevant jurisdiction in application of Article 8 of the General Data Protection Regulation ("GDPR")).

reports to help monitor device use. Parents can use Screen Time to better understand and make choices about how much time their children spend using apps and websites. Activity Reports give parents a detailed overview of their child's app usage, notifications, and device pickups – and only they, their children, and those they choose to share it with can view this information. Parents can choose to apply content restrictions, which restrict download of, for example apps or games with specific age ratings or categories of apps or games. They can also fully restrict the downloading of some or all apps via Screen Time settings.

3.4.5 Further, through Screen Time, parents can set individual parental controls to restrict their children's Apple devices to limit the websites they visit, the types of movies and TV shows they watch, their access to FaceTime and Camera, and the types of music and podcasts they can access, to prevent them encountering explicit content. All this can be password protected with a parental code. Parents can also place restrictions on privacy settings, such as for Location Services and Photos, so that their children cannot change those settings themselves. Apple facilitates parents to make exceptions for specific apps, like educational or mindfulness apps and even allows parents to set specific times during the day when apps, notifications and certain features are automatically blocked. Parents can also select which apps appear on their child's device "home" screen.

3.4.6 Communication Limits 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.

3.4.7 Ask to Buy allows parents to approve app downloads and purchases requested by the child, including in-app purchases, on the App Store or otherwise using iTunes. It is enabled by default for any children under 13 and can be enabled for any family member under 18 by the Family Organiser.[12]

3.4.8 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 App Store will complete the download or purchase on the child's device. If they decline, the process stops there (i.e. App Store will not complete the download or purchase).

### *(b) Child protection*

3.4.9 Communication Safety is a parental control feature which provides warnings in the event that a child receives or sends images containing nudity on iMessage. From the next OS update (e.g. iOS 17), this feature will be enabled by default for all users under 13 years of age or equivalent minimum age in their country or territory of residence. Parents can also enable the feature via Family Sharing for children under 18 years of age. By using an on-device image classifier, the image is detected and blurred and the child receives an alert along with helpful and age-appropriate resources and the option to send a message to a trusted person for help. This feature is to be expanded

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

to Airdrop and FaceTime video messages, as well as PhotosPicker. It will also be made available to developers for use on third-party messaging and communication apps by implementing the Sensitive Content Analysis framework (starting with iOS 17).[13] End-to-end encryption is maintained and no one, including Apple, has access to the messages.

3.4.10 Expanded guidance in Siri and Safari search provides additional online safety information and local resources, which includes information on how to report Child Sex Abuse Material ("CSAM") or Child Sexual Exploitation and Abuse ("CSEA") and how to seek support and advice for situations which may arise online and offline (helplines and hotlines in each jurisdiction). Siri and search will also intervene in the event that users perform searches for CSAM, explaining the dangerous and illegal nature of it and providing resources and links to partners who can provide help to prevent abuse.

3.4.11 Within Apple's Global Security function, 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.

### *(c) Children and data*

3.4.12 Apple understands the importance of safeguarding the personal data of children. That is why Apple has implemented additional processes and protections for children. If Apple learns that a child's personal data was collected without appropriate authorisation, it is deleted as soon as possible.

3.4.13 Apple maintains robust privacy protections as a basic requirement for all of its users, including children, ensuring the provision of strong safeguards to all children regardless of their age range or developmental stage. These high standards include data-minimisation, on-device processing, transparency measures, and data security tools.

3.4.14 Additional App Store-specific controls relevant to children are addressed in Section 6 of this Report.

## 3.5 Human rights

3.5.1 Apple is committed to respecting human rights, including the right to privacy and freedom of information and expression. Human rights are at the core of how Apple treats everyone – from its customers and teams to its business partners and people at every level of its supply chain. Apple reflected this commitment in its Human Rights

[13] https://developer.apple.com/documentation/sensitivecontentanalysis

policy, first published in 2020,[14] which states that Apple's approach to human rights issues is based on the UN Guiding Principles of Business and Human Rights. The Policy was adopted by Apple Inc.'s Board (the "Apple Inc. Board"), which is responsible for overseeing and periodically reviewing it. Apple's Senior Vice President and General Counsel oversees the implementation of this Policy and reports to the Apple Inc. Board and its committees on progress and significant issues.

3.5.2 The Human Rights Policy touches on a number of issues that are relevant to Apple, including human rights considerations in the design and functioning of its products and human rights risks in its supply chains, and explains that, in keeping with the UN Guiding Principles, where national law and international human rights standards differ, Apple follows the higher standard. Where they are in conflict, Apple respects national law while seeking to respect the principles of internationally recognised human rights.

3.5.3 Apple has a dedicated Human Rights function that is responsible for conducting human rights due diligence across Apple, in order to identify human rights risks arising in connection with Apple's business operations and to implement plans to prevent or mitigate such risks. It also works with different business groups to align existing processes with the Human Rights Policy framework. In addition, the team issues human rights-related training content, which is delivered to Apple employees around the globe.

3.5.4 Apple identifies salient human rights risks through internal risk assessments. In some cases, it identifies issues via external industry-level third-party audits, as well as through the channels it maintains with rights holders and other stakeholders, including investors, human rights and labour experts, governments, and international bodies such as the UN. In addition to its own internal monitoring, Apple considers reports identifying potential risks from external sources, including international organisations, policy makers, shareholders, civil society organisations, news outlets, customers, individuals in the supply chain or supply chain communities, whistleblower mechanisms, and third-party hotlines.

3.5.5 Based on this type of due diligence, by way of example, in 2022 Apple identified the following human rights issues of particular focus (detailed in its 2022 Environmental Social Governance ("ESG") Report):[15]

(a) Privacy, freedom of expression and access to information risks;

(b) Discrimination risks in workforce management and in product services and development; and

(c) Labour and human rights risks in the supply chain.

3.5.6 More detail on Apple's ongoing human rights efforts are detailed in the 2022 ESG Report.

[14] https://s2.q4cdn.com/470004039/files/doc_downloads/gov_docs/2020/Apple-Human-Rights-Policy.pdf

[15] https://s2.q4cdn.com/470004039/files/doc_downloads/2022/08/2022_Apple_ESG_Report.pdf

### 3.6 Apple fraud prevention

3.6.1 Apple employs industry best practices to safeguard Apple customers and prevent potentially fraudulent transactions, across Apple Media Products platforms, including for example the App Store, Apple Music, and iCloud services.

3.6.2 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.

3.6.3 Apple has also developed an internal set of proprietary risk tools allowing Apple to review data to comprehensively understand the effects of its fraud detection efforts and propose new approaches to fraud attempts. These tools include monitoring mechanisms that utilise AI/ML techniques which aid Apple in being flexible and adaptable in its current and future fraud detection efforts. Risk decision tools are evaluated for their impacts on fraud reduction and adjusted periodically to ensure Apple is making the most of its available tools and detection methods.

3.6.4 In 2020, Apple's combination of technology and human expertise protected customers from more than $1.5 billion in potentially fraudulent transactions. In 2021, Apple protected customers from nearly $1.5 billion in potentially fraudulent transactions, and stopped more than 1.6 million risky and vulnerable apps and app updates from defrauding users.[16] In 2022, Apple blocked nearly 3.9 million stolen credit cards from being used to make fraudulent purchases, and banned 714,000 accounts from transacting again. In total, in 2022, Apple blocked $2.09 billion in fraudulent transactions on the App Store.[17]

[16] https://www.apple.com/newsroom/2022/06/app-store-stopped-nearly-one-point-five-billion-in-fraudulent-transactions-in-2021/

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

## SECTION 4: THE RISK PROFILE OF THE APP STORE

### 4.1 Section overview

4.1.1 The DSA identifies, in broad terms, categories of potential Systemic Risk and factors for VLOPs to consider in assessing such risks. The DSA also recognises that each VLOP's risk assessment should be tailored to the unique "*design or functioning of their service and related systems*" and "*shall be specific to their services and proportionate to the systemic risks*" of that service.[18] This recognises that each VLOP will have its own distinct risk profile and assessment based on the design, functioning and use of its service.

4.1.2 The App Store[19] provides users of Apple devices with the means to discover and download apps from the App Store. From its inception, the App Store was designed to protect users of Apple devices by creating a safe and trusted environment offering a wide variety of curated apps. Every app and every app update submitted to the App Store is closely reviewed by both automated systems and human experts trained to ensure that apps offered on the App Store are safe, provide a good user experience, protect user privacy, and use approved business models. Post publication, apps are subject to ongoing monitoring and multiple controls ensure that Apple can take action when it is alerted to problematic developers or apps. However, Apple cannot monitor all activity that happens within the app given Apple's privacy by design principles, which means that the apps run on the device so as to minimise the data shared with Apple.

4.1.3 This Risk Assessment addresses the potential systemic risks of the App Store that exist within the framework of the lifecycle of an app distributed in the App Store. Risks that arise outside of the App Store are beyond the scope of Article 34. As such, this Section provides an overview of the lifecycle of an app in the App Store – including app discovery, where users learn about and download apps. This Section also summarises the stages before app discovery: developer onboarding; app review; and recommender, advertising, and moderation systems that impact the presentation of apps and reviews to customers. Finally, this Section addresses the App Store's notice and action mechanisms, which help to mitigate potential App Store risks, as well as external risks that are the responsibility of developers.

4.1.4 Note that this Section describes how users discover Apps in the App Store service, and the process by which apps are published on the App Store, and notices and

[18] Digital Services Act, Article 34(1).

[19] As noted at footnote 1 above, ADI does not accept that iOS App Store, iPadOS App Store, watchOS App Store, macOS App Store and tvOS App Store all form part of a single online platform. Rather, they are separate online platforms with significant differences from both a developer and end user perspective. Notwithstanding this, several of the key compliance controls forming part of Apple's risk mitigation measures under Article 35 of the DSA apply to each of the current App Stores. As such, in this risk assessment, save as indicated otherwise, or where obvious from context, use of the expression "App Store" should be understood as extending to each of iOS App Store, iPadOS App Store, watchOS App Store, macOS App Store and tvOS App Store.

actions measures, to guide the reader when considering the Systemic Risk assessment in Section 5. Detailed information regarding the risk mitigation controls mentioned in this Section 4 and their role in mitigating the Systemic Risks is provided in Section 6.

## 4.2 The App Store provides app discovery and distribution

4.2.1 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.[20]

4.2.2 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.

4.2.3 The App Store operates 175 country- or region-specific "storefronts", and users transact through a storefront based on their home country. Each EU Member State has a separate storefront.[21] The App Store is available in 40 languages, including 17 official languages of the EU.[22] Information presented in the App Store is therefore "localised", such that app metadata[23] is displayed in different languages, depending on a user's location and language settings. Editorially curated content (described below) may vary, depending on a user's location.

### *(a) The "Today" tab*

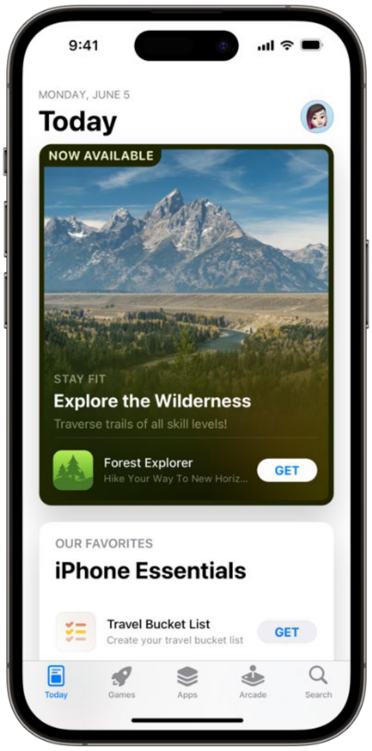
4.2.4 The Today tab is the first page a user sees when they click on the App Store icon on their device. Apple considers this a "daily destination" with original stories from App Store editors, featuring exclusive premieres, new app releases, Apple's all-time favourites apps, an "App of the Day", a "Game 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.

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

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

[22] https://developer.apple.com/localization/

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



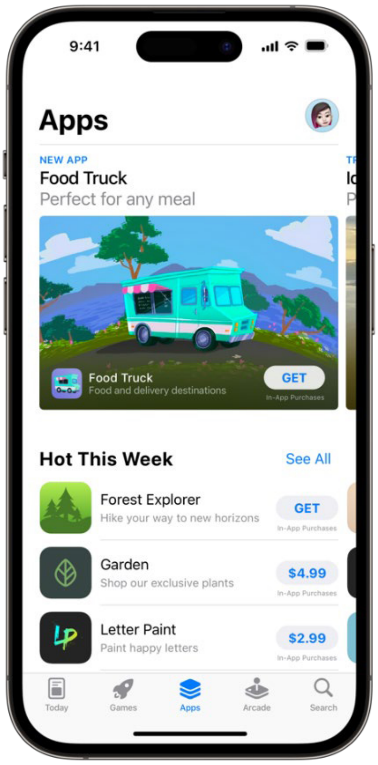
4.2.5 App Store editors create a curated catalogue of apps for each category in the Today tab (for example, original stories, tips, how-to guides, interviews, App of the Day, Game of the Day, Now Trending, Collections, Our Favourites, Get Started). For each curated category, the Editorial team determines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

4.2.6 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.

4.2.7 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.

### *(b) <u>The "Games" and "Apps" tabs</u>*

4.2.8 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.



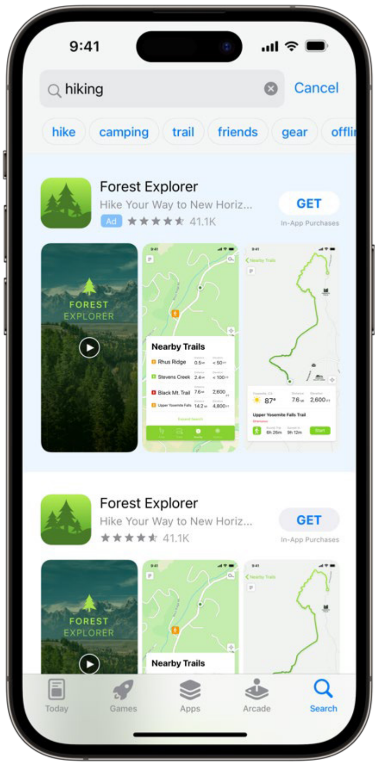
4.2.9 When considering apps to feature in these tabs, App Store editors look for high-quality apps across all categories, with a particular focus on new apps and apps with significant updates.

### *(c) <u>"Arcade" tab</u>*

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

### *(d) <u>Search tab</u>*

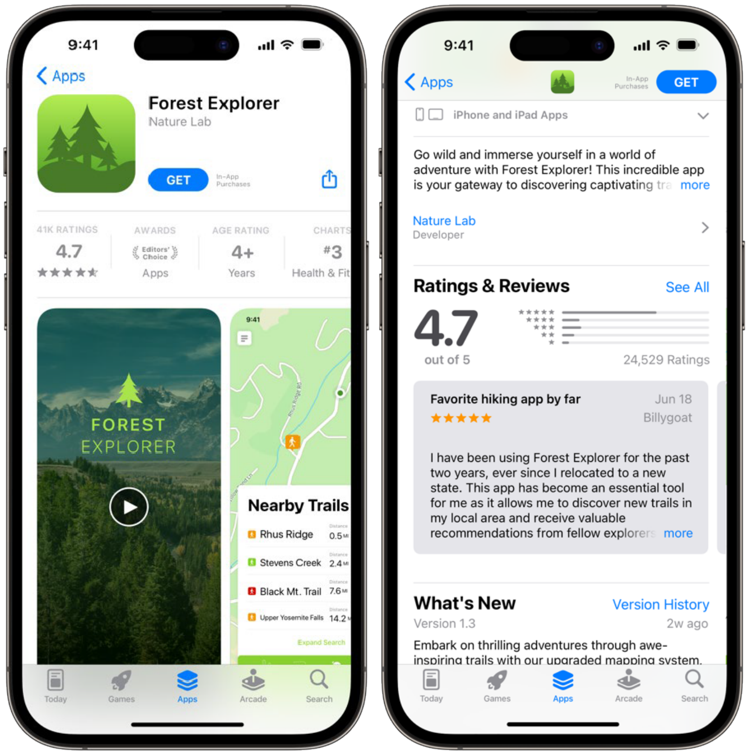
4.2.11 The App Store Search tab provides an additional way for customers to find apps, games, stories, categories, in-app purchases, and developers. Before a user enters a search, the Search tab shows popular or trending queries in the "Discover" section, as well as a list of apps that a user may want 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.



4.2.12 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.

### *(e)* *App product page*

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



Go wild and immerse yourself in a world of adventure with Forest Explorer! This incredible app is your gateway to discovering captivating tra more

I have been using Forest Explorer for the past two years, ever since I relocated to a new state. This app has become an essential tool for me as it allows me to discover new trails in my local area and receive valuable recommendations from fellow explorers more

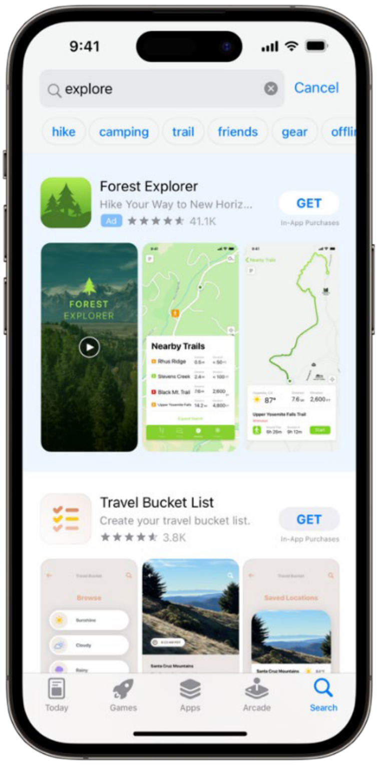
Embark on thrilling adventures through awe-inspiring trails with our upgraded mapping system.

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

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

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

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



4.2.17 Apple Search Ads is a purely optional service for developers, accessible through an independent account (an Apple Search Ads account), using a different web portal from App Store Connect.[24] Apple Search Ads were made available to users in certain EU storefronts five years ago; more were added thereafter.[25] Today, Apple Search Ads are available to users in most EU storefronts,[26] though only a small percentage of App Store developers choose to promote their apps using Apple Search Ads. If developers choose to not use the Apple Search Ads service to promote their app, their app will still appear across the various available organic placements of the App Store, including within search results, just as it would if the developer had chosen to use Apple Search Ads for securing promoted placements. The two services and placement algorithms work separately from each other.

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

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

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

[25] https://searchads.apple.com/countries-and-regions

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

### *(a) Developers are screened and must agree to terms and conditions*

4.3.2 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,[27] 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.

4.3.3 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 appear to intend to commit serious breaches of the Apple Developer Agreement (the "ADA"), DPLA or App Review Guidelines) and associates do not re-enter the program. In addition, the global export sanctions compliance team also conducts a sanctions check against the developer information to ensure Apple is not prohibited from doing business with the developer.

4.3.4 If a developer passes this round of screening, they can then execute the DPLA,[28] and begin the multi-step process of submitting an app for distribution on the App Store.

### *(b) Automated and human-based app review*

4.3.5 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).

4.3.6 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.[29] Every app or app update submission is then reviewed by the App Review team, first via automated means and then by human app reviewers.

4.3.7 The App Review automated process includes static binary analysis, asset analysis, and runtime analysis [CONFIDENTIAL]. The aim of these automated processes is to efficiently gather information that can be interpreted by machine learning algorithms and analysed for threats and signals (for example, the presence of malicious URLs or executable code) that provide relevant app information to the human review component.

4.3.8 During human review, app reviewers analyse the signals provided by automated systems and review the features and functionality of apps to ensure they are

[27] https://developer.apple.com/support/downloads/terms/apple-developer-agreement/Apple-Developer-Agreement-20230605-English.pdf

[28] https://developer.apple.com/programs/apple-developer-program-license-agreement/

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

compatible with the App Store's systems and products, comply with the Guidelines, and do not give signs of potential deceptive, abusive, or otherwise harmful behaviour. If a reviewer detects a potential Guideline violation, they engage with the developer, reject the app or further escalate issues to specialists within the App Review team or to other functional groups, such as the App Store Legal team. If there are no Guideline violations, the app may be approved for publication in the App Store.

### *(c) <u>Post-publication review</u>*

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

### *(d) <u>[CONFIDENTIAL]</u>*

4.3.10 [CONFIDENTIAL].

### *(e) <u>Reviews of user-generated ratings and reviews of apps</u>*

4.3.11 The only UGC on the App Store is user-generated app ratings and reviews, both of which are subject to content moderation by the Trust and Safety Operations team. The Trust and Safety Operations team takes both preventative and responsive steps to ensure that risks arising from ratings and reviews are minimised. These risks may include inauthentic or misleading ratings and reviews, including by users who have not used the app.

4.3.12 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.

(f) ***For apps live on the store, the App Store provides avenues for consumers, developers, government authorities and others to provide notice of potential problems or concerns with apps or app content***

4.3.13 Customers may use the "Report a Problem" feature to submit notices of offensive, illegal, or abusive content concerning apps they have purchased or downloaded. Report a Problem is accessible via quick links at the bottom of the Games and Apps tabs or from the product page of any app purchased or downloaded. These submissions are screened for manipulation and, if legitimate, forwarded to the appropriate team (for example, the App Review team, or Trust and Safety Operations) to investigate for signs of fraud, manipulation, abuse and other violations of the Guidelines and take action, if necessary. Such action may include working with developers to resolve issues, removing illegal or harmful apps, and / or terminating developer accounts. As detailed in Section 6, developers have recourse to various appeal mechanisms in the event that they disagree with Apple's decision to remove apps or terminate developer accounts.

4.3.14 Developers and users also have the ability to report potential problems or concerns with app reviews or ratings by submitting notices using Apple's "Report a Concern" function. [30] This feature allows developers to submit a customer review removal request, and for developers and users to report concerns with user ratings and reviews, including concerns regarding relevance, spam or fraud. As with customer Report a Problem notices, developer and user notices regarding ratings and reviews are forwarded to the appropriate internal teams for review, investigation, and potential action.

4.3.15 If a developer or user believes that an app violates their intellectual property rights, they can submit a claim to the AMS Content Disputes Legal team, using the App Store content disputes form.[31] The team will put them in direct contact with the developer, as primary responsibility for settling content disputes rests with the parties. In some circumstances, the AMS Content Disputes Legal team will intervene and take action against developers and apps.

4.3.16 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.

4.3.17 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.

[30] https://developer.apple.com/contact/#!/topic/select/SC1108/subtopic/select

[31] https://www.apple.com/legal/internet-services/itunes/appstorenotices/#?lang=en

4.3.18 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.

### *(g) New DSA Notices and Actions Process*

4.3.19 In August, pursuant to its DSA obligations, Apple made updates to the Report a Problem process and introduced a new content reports portal.

4.3.20 Users on a storefront in the EU now have the option to select "Report offensive or abusive content" or "Report illegal content" from the options menu. If the user selects "Report offensive or abusive content" the process remains as described in paragraph 4.3.13 above. If they select "Report illegal content", they are redirected to a web portal at ContentReports.apple.com (the "Content Reports portal"). The Content Reports Portal can also be accessed directly via the web.

4.3.21 The Content Reports portal is a central platform where individuals, including government representatives, and in due course "Trusted Flaggers"[32], 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.

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

## SECTION 5: POTENTIAL SYSTEMIC RISKS ARISING FROM THE DESIGN, FUNCTIONING OR USE OF THE APP STORE

### 5.1 Section overview

5.1.1 This Section contains an assessment of how the Systemic Risks in the EU may stem from the design, functionality or use of the App Store.[33]

5.1.2 Following careful analysis, Apple has not identified any meaningful basis to distinguish risks stemming from the design and function of the App Store from risks stemming from its use. The App Store controls environment has been developed over many years in a manner designed to address issues arising from the way in which the App Store is used by developers and end users. Against that background, and to avoid unnecessary and unhelpful artificiality and repetition, Apple has sought to identify risks as they may arise from the design and function of the App Store, taking into account its use.

5.1.3 While the concept of Systemic Risk is not comprehensively defined in the DSA, Apple has not identified any risks in the EU beyond or separate from those listed in Article 34(1) that might reasonably be said to stem from the design and function of the App Store, or its use, and that might reasonably be said to be systemic in nature. As such, this risk assessment addresses those Systemic Risks specifically identified in Article 34(1).

### 5.2 Article 34(2) first paragraph factors

5.2.1 Pursuant to Article 34(2) first paragraph, in conducting this risk assessment, Apple is required to take account of whether and how certain specified factors may influence any of the Systemic Risks. Each of the factors are considered in Section 6 of the Report, but Apple notes the following:

#### *(a) Recommender systems and other algorithms*

5.2.2 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.

5.2.3 As detailed in Section 6 (in particular, paragraphs 6.6.1 *et seq.* below), while Apple makes limited use of recommender and other algorithmic systems compared with other VLOPs, 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. Furthermore, the App Store recommender function makes no use of profiling. 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 children's accounts, where recommendations cannot be personalised).

[33] The assessment of risks in this Section is limited to those risks that may arise in the EU.

5.2.4 Additional controls detailed in Section 6 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. As such, the impact of this factor on Systemic Risks is taken into account throughout this risk assessment.

### *(b) Content moderation systems*

5.2.5 Prior to the passing of the DSA, there were already various content moderation systems on the App Store, including ongoing monitoring of apps on the App Store as well as moderation of user ratings and reviews and developer responses (as explained at paragraphs 6.7.1 *et seq.* below). The impact of these systems on the Systemic Risks is detailed in relevant sections of the Report. Furthermore, Apple requires developers whose apps allow UGC to maintain effective content moderation arrangements. While the significance of UGC on the App Store is dramatically lower than as regards some other VLOPs, content moderation is considered in all relevant sections of this risk assessment.

### *(c) Applicable terms and conditions*

5.2.6 Apple maintains comprehensive terms and conditions – applicable to both developers and 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 user misuses the App Store. Developers and users who object to such action have recourse to various complaints mechanisms.

5.2.7 These terms and conditions, and the ways in which they and their enforcement facilitates Apple's mitigation of Systemic Risks, are addressed extensively throughout this risk assessment.

### *(d) Systems for selecting and presenting advertising*

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

5.2.9 As detailed in Section 6, the only developer promotion of an app on the App Store appears in Apple Search Ads. These are 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. As such, Apple does not consider that Apple Search Ads can to any meaningful extent be reasonably or objectively said to be a catalyser for the Systemic Risks.

5.2.10 Apple further notes that Recital 79 to the DSA suggests that the way in which VLOPs "design their services is generally optimized to benefit their often advertising-driven business models and can cause societal concerns." Although certain VLOPs may design their services in this way, it is certainly not the case for the App Store, where Apple Search Ads only provides developers an opportunity to promote their apps and not to "advertise" additional content. The promoted apps have already been reviewed and approved for the App Store.

### *(e) Data-related practices of the provider*

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

5.2.12 This risk assessment, including the assessment of the Charter right to the protection of personal data at paragraph 5.7.13 *et seq.* below, addresses extensively all relevant privacy and data protection considerations, including those that apply at the Apple ecosystem level, and those specific to the App Store.

## 5.3 Intentional manipulation of the App Store

5.3.1 Furthermore, 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. In this regard, Recital 84 provides that:

> *"... Providers of very large online platforms ... should, in particular, assess how the design and functioning of their service, as well as the intentional and, oftentimes, coordinated manipulation and use of their services, or the systemic infringement of their terms of service, contribute to such risks. Such risks may arise, for example, through the inauthentic use of the service, such as the creation of fake accounts, the use of bots or deceptive use of a service, and other automated or partially automated behaviours, which may lead to the rapid and widespread dissemination to the public of information that is illegal content or incompatible with an online platform's ... terms and conditions and that contributes to disinformation campaigns."*

5.3.2 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.

## 5.4 Regional or linguistic aspects

5.4.1 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.

5.4.2 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. 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 may be required by law. Nonetheless, where appropriate in Section 6 below, we refer to regional or linguistic considerations within the EU.

## 5.5 The Systemic Risks and the App Store

5.5.1 Given the integrated nature of the risk mitigation measures implemented and enhanced by Apple since the launch of the App Store, seeking to identify the systemic risk profile without reference to all mitigation measures inevitably involves some artificiality. Apple recognises that without effective controls any app store, including the App Store, could be open to serious abuse by malicious actors that could engage the Systemic Risks. Since its inception, the guiding principle of the App Store has been to maintain a safe and trusted place for end users to discover and download apps, and extensive controls are in place to ensure that the apps that are offered on the App Store are held to the highest standards for privacy, security, safety and quality. Apple has taken and continues to take steps to keep the App Store a safe place, and to give users control over their preferences, irrespective of any legislative initiatives, such as the DSA.

5.5.2 Apple directly mitigates risks from apps or UGC on the App Store. Developers and consumers are nearest to the source and primarily mitigate risks that arise outside of the App Store. For those risks, developers must engage in risk mitigation measures (such as their own content moderation systems). While Apple's privacy by design principles mean that Apple cannot carry out an on-going review of UGC in the app, Apple considers that it is critical for the integrity of its ecosystem to invest in the mitigation of those risks, as well, including by making extensive tools available to developers and consumers for those purposes and by requiring developers to maintain certain safeguards in accordance with the DPLA and the Guidelines. Apple also conducts ongoing App Review to help mitigate even those risks which are outside of Apple's control, as set out further below in Section 6. Such comprehensive controls which comprise the security architecture of the App Store are necessary to effectively mitigate risks throughout the lifecycle of an app distributed via the App Store.

5.5.3 However, those risks which do not stem from the design or function of the App Store, or from its use (as opposed to the use of such third-party apps), are extraneous to the App Store. Developers have responsibilities to mitigate risks to users (including those required by Apple under the DPLA), and those which are themselves VLOPs will have their own new risk mitigation measures under the DSA. Risks arising from the design, function or use of their services are not the responsibility of Apple; although they may engage obligations owed to Apple under the DPLA, and are subject to the App Review process.

5.5.4 If Apple identifies through App Review or is alerted to content on third-party apps downloaded on a user's device that engages the Systemic Risks, its practice is to mitigate those risks as efficiently as practicable. Apple typically first brings such matters to the attention of the app developer so that they can take action. In the event that the developer fails to take appropriate action, Apple can take measures to prevent further distribution via downloads or re-downloads from the App Store, but those actions are in response to risks that stem from use of third-party apps, not use of the App Store, and are therefore independent of any liability under the DSA.

5.5.5 In this Section of this report, in assessing each of the Systemic Risks specified in Article 34(1), and in considering probability of such risks arising and the severity of any resulting impacts, Apple has sought to take into account the level of inherent risk, without regard to the extensive App Store risk mitigation measures that address the risk in question, save to the extent that it would be wholly artificial to do so, given that many of the risk mitigation measures are so integral to the way the App Store operates, and so fundamental to its design. Those mitigation measures are addressed in Section 6.

## 5.6 Article 34(1)(a) – Dissemination of illegal content

5.6.1 "Illegal content" is defined in the DSA as "*any information that, in itself or in relation to any activity including the sale of products or the provision of services, is not in compliance with Union law or the law of any member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law*". Recital 80 of the DSA provides, as examples of "illegal content", child sex abuse material or illegal hate speech or other types of misuse of the service for criminal purposes and the conduct of illegal activities. Such dissemination may become a significant systemic risk "*where access to illegal content may spread rapidly and widely through accounts with a particularly wide reach or other means of amplification.*"[34] Apple notes that amplification or proliferation of content (which may contain illegal content) does not form part of the business model of the App Store.

[34] Recital 12 further provides that "*In order to achieve the objective of ensuring a safe, predictable and trustworthy online environment, for the purpose of this Regulation the concept of 'illegal content' should broadly reflect the existing rules in the offline environment. In particular, the concept of 'illegal content' should be defined broadly to cover information relating to illegal content, products, services and activities. In particular, that concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that the applicable rules render illegal in view of the fact that it relates to illegal activities. Illustrative examples include the sharing of images depicting child sexual abuse, the unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the sale of products or the provision of services in infringement of consumer protection law, the non-authorised use of copyright protected material, the illegal offer of accommodation services or the illegal sale of live animals. In contrast, an eyewitness video of a potential crime should not be considered to constitute illegal content, merely because it depicts an illegal act, where recording or disseminating such a video to the public is not illegal under national or Union law. In this regard, it is immaterial whether the illegality of the information or activity results from Union law or from national law that is in compliance with Union law and what the precise nature or subject matter is of the law in question.*"

### *(f)* *Developer content*

5.6.2 As with any online platform, there is a material risk that, absent risk mitigation measures, the App Store could be used to disseminate certain categories of illegal content to users in the EU. This could include, without limitation:

(a) apps designed to disseminate illegal content or facilitate illegal behaviours, such as fraud, including "bait-and-switch" apps;

(b) apps that infringe the intellectual property rights of others;

(c) apps that facilitate activities that are illegal in certain Member States (for example, certain types of real money gambling);

(d) in-app content that is defamatory or intended to offend; or

(e) developer responses to user reviews that are intended to mislead or induce improper behaviours.

5.6.3 However, the App Store developer screening measures, App Review process, content moderation practices and notices and actions procedures are designed to and do minimise the potential for dissemination of illegal content or the use of the service for unlawful purposes, and seek to swiftly identify any such content or behaviours at the earliest possible juncture so as to minimise the possibility of their amplification.

5.6.4 Notwithstanding these controls, as noted above, malicious actors are, in practice, constantly trying to evade the App Store's controls, including through inauthentic use and intentional manipulation of the App Store; in that sense, this Systemic Risk does arise in practice. The App Store 2022 Transparency Report provides some insight into the scale of the threat. In 2022, the App Store rejected 1,679,694 apps / app updates for safety and legal reasons; it removed 186,195 apps for fraud, IP infringements, Copycats, and other legal reasons.

5.6.5 As such, absent appropriate controls, the risk of the App Store being used to disseminate illegal content would be high, and, depending on the type of illegal content, the severity of impact of such risk crystallising could range from moderate to extreme (such as in the case of terrorist content or CSAM). However, the App Store maintains risk mitigation measures to address these risks.

### *(g)* *User content*

5.6.6 The only UGC on the App Store (as opposed to content generated by developers; and UGC within third-party apps) appears in user ratings and reviews of apps available on the App Store.

5.6.7 The risk that App Store-hosted UGC may give rise to the dissemination of illegal content is low to moderate, and most likely to arise through offensive statements, defamation, harassment, and potentially through co-ordinated disinformation or fraudulent campaigns in favour of or against a particular app or developer. However, the limited presence of UGC and distribution thereof makes the App Store a significantly less likely target of such practices, compared with other platforms.

Furthermore, Apple moderates all 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.

### 5.7 Article 34(1)(b) – Actual or foreseeable negative effects for the exercise of fundamental rights

5.7.1 Article 1 of the DSA provides that its aim is to "*contribute to the proper functioning of the internal market for intermediary services by setting out harmonised rules for a safe, predictable and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected.*"

5.7.2 Recital 81 of the DSA provides that VLOPs must assess the "*impact of the service on the exercise of fundamental rights*". It explains that:

> "*Such risks may arise, for example, in relation to the design of the algorithmic systems used by the [VLOP…] or the misuse of their service through the submission of abusive notices or other methods for silencing speech or hampering competition. When assessing risks to the rights of the child, providers of [VLOPs…] should consider for example how easy it is for minors to understand the design and functioning of the service, as well as how minors can be exposed through their service to content that may impair minors' health, physical, mental and moral development. Such risks may arise, for example, in relation to the design of online interfaces which intentionally or unintentionally exploit the weaknesses and inexperience of minors or which may cause addictive behaviour.*"

5.7.3 The App Store is primarily a vehicle for the promotion and fulfilment of fundamental rights, in particular freedom of expression and information, offering developers opportunities to distribute their apps to the users of Apple devices, and those users to discover and download apps.

5.7.4 Apple notes that human app reviewers on the App Review team are trained to review apps with a view to identifying potential human rights concerns. For example, with a view to safeguarding individuals and users, human reviewers examine each and every app and each and every app update submitted for App Review against the terms of the Guidelines that clearly prohibit app content that is "*offensive, insensitive, upsetting, intended to disgust…*", including "*references to commentary about religion, race, sexual orientation or other targeted groups…*".

5.7.5 Apple considers that any Charter Rights risks associated with the design, function or use of the App Store primarily are those set out below.

#### *(h) Rights to human dignity and respect for private and family life, enshrined in Articles 1 and 7 of the Charter*

5.7.6 Use of the App Store is capable of engaging (and therefore conceivably capable of giving rise to negative effects) the right to human dignity in Article 1 and the right to respect for private and family life in Article 7. Given the close relationship between those rights, and the ways in which they may be engaged in connection with the App Store, they are considered together for the purposes of this risk assessment.

5.7.7 Developer use of the App Store may engage these rights where apps are submitted with relevant malign intent, or containing illicit app binary functionality, or lacking the controls required for apps of the relevant kind by the Guidelines (such as, for example, an app encouraging UGC which is not supported by appropriate content moderation measures).

5.7.8 Absent adequate controls, the likelihood of developers seeking to publish apps capable of giving rise to actual or foreseeable negative effects on the rights to human dignity and respect for private and family life would be high, and the severity of such risks could vary from modest to extreme (for example, in the cases of CSAM, so-called "revenge pornography", "deepfakes", etc.); indeed, in practice, action does from time to time have to be taken to block or remove apps containing such content. Nonetheless, the App Store maintains risk mitigation measures to address these risks.

### *(i) Developers' and users' rights to the protection of personal data enshrined in Article 8 of the Charter*

5.7.9 The right to protection of personal data is closely associated with the right to privacy and the right to human dignity.

5.7.10 When users interact with an app store via their device, the app store provider can collect and process their personal data in a number of different ways. This could include profiling their user behaviour in the application store, including by tracking their browsing and searching activities, and processing their personal data for presenting recommended apps and other content, including advertising material. App store providers could also share this personal data with third parties, including data brokers.

5.7.11 Without appropriate risk mitigation measures on the App Store, there would be a significant risk that there could be negative effects on developers' and users' rights to the protection of their personal data.

5.7.12 However, as detailed in Section 3 above (in respect of Apple ecosystem privacy practices) and Section 6 below (in respect of App Store specific privacy practices), the App Store maintains comprehensive policies relating to privacy and data protection, and uses on-device processing to enhance recommendations and mitigate privacy risks.

### *(j) The rights of developers and users to freedom of expression and freedom of information, including the freedom and pluralism of the media, under Article 11 of the Charter*

5.7.13 Developers' and users' rights to freedom of expression and information are engaged when they interact with the App Store. Nonetheless, Apple recognises that there is a balance to be struck between freedom of expression and other rights and interests which might be adversely affected by untrammelled exercise of free expression (for example, rights to dignity, privacy, and freedom from discrimination). The Introduction to the Guidelines reflects the App Store's approach:

> "*We strongly support 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 great. We will reject apps for any content or behavior that we believe is over the line. What line, you ask? Well, as a Supreme Court Justice once said, "I'll know it when I see it". And we think that you will also know it when you cross it.*"

5.7.14 Developers and users are free to use the App Store, save where they do not comply with the law or the Guidelines, which are designed to keep the App Store a safe and trusted place for all. Each of the rights to freedom of expression and information is susceptible to proportionate limitation, which is the purpose and effect of the Guidelines, and the risk mitigation measures applicable to the App Store generally. As such, while such risks may conceivably arise in connection with the App Store, the probability of negative effects on these rights arising in practice can only reasonably be seen as remote; and their impact, should they arise, modest. In any event, where developers and users disagree with Apple's decisions that could engage freedom of expression and information, there are complaints processes available to address such concerns.

5.7.15 Recital 81 of the DSA refers to freedom of expression or information being threatened by misuse, including the submission of "*abusive notices or other methods for silencing or hampering competition*". In the context of the App Store, this risk can arise in the context of abusive challenges to published apps or improper or bad faith ratings and reviews about an app submitted by competitors. This risk may arise from developer or end user use of the App Store. App Store controls are designed to and do protect against these risks.

5.7.16 The App Store is a vehicle for media pluralism across the EU, counting among its developers a very wide range of media voices. The App Store is not a news service or news aggregator. Media apps are available on the App Store unless illegal or otherwise in breach of the Guidelines. While the risk of repressive governments seeking to abuse powers to require takedown of apps or content cannot be discounted, in practice, the prevalence of such behaviour within the EU is low (albeit, non-negligible), and would be subject to legal challenge with strong prospects of success under domestic rights norms in the Member States, informed by the European Convention on Human Rights.

5.7.17 Apple notes that in its November 2022 Discussion Document on Media plurality and online news,[35] Ofcom, the UK's Office of Communications, makes no mention of the App Store, which tends to corroborate the view that any risks of negative impacts on media pluralism stemming from the design, function or use of the App Store are low. Apple has also not identified any commentary from the European Parliament or

[35] https://www.ofcom.org.uk/__data/assets/pdf_file/0030/247548/discussion-media-plurality.pdf

European Commission that refers to the App Store giving rise to a systemic risk to media plurality in the EU.

### *(k) The right to non-discrimination under Article 21 of the Charter*

5.7.18 Article 21 of the Charter provides that discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited. Article 21(2) of the Charter also imposes a prohibition on discrimination based on nationality.

5.7.19 In principle, an app store could discriminate against users or developers on prohibited grounds when granting them access to the service, when reviewing whether apps will be published on the service, or when determining which apps will be made available to them.

5.7.20 Apple does not discriminate against developers or users, including when conducting developer screening, App review, or responding to notices and actions (including from law enforcement).

5.7.21 As regards app recommendations and Apple Search Ads, if a user has personalisation turned on, age, gender and location are used to present personalised content, but such conduct does not amount to discrimination (and in any event ad personalisation can be switched off).

5.7.22 As regards developer use, although discriminatory content is clearly prohibited under the Guidelines, there is a risk that users could be exposed to such content in the App Store if it were not identified during the App Review process. However, app reviewers are trained to identify such content, and the notices and actions and complaints mechanisms provide means to raise relevant concerns regarding apps that are already published on the App Store.

### *(l) The freedom to conduct a business under Article 16 of the Charter (to the extent that a developers' apps must follow the rules of the App Store)*

5.7.23 For the purposes of this risk assessment, Apple has considered whether a developer's rights to freedom to conduct a business could conceivably be negatively affected if they were prevented without justification from distributing apps on the App Store, or the developer were terminated or its apps taken down without justification.

5.7.24 While this right could conceivably be engaged in such circumstances, a number of factors indicate that the probability of negative impacts on the enjoyment of this right arising in practice is low, and the severity of impacts modest:

(a) First, the right under Article 16 does not imply a right to enter into contractual relationships with any given counterparty;

(b) Second, any engagement of this right through developer termination or restrictions on apps would be substantially mitigated by the existence of numerous other platforms and other media on which apps may be published and distributed;

(c) Third, under the Charter, this freedom is susceptible to proportionate limitation, which is the purpose of the App Store risk mitigation measures generally; and

(d) Fourth, developers have at their disposal numerous options for contesting unfavourable decisions relating to the publication of apps on the App Store, including an internal appeals process, mediation vehicles (such as through the mechanism afforded under the Platform-to-Business Regulation [36] ) and the courts.

5.7.25 As such, while a developer's business may be affected by a decision on Apple's part, it does not follow that the developer's right under Article 16 is engaged by such a decision; and even were it accepted that the right could be engaged, any concerns arising under this Article can only reasonably be seen as highly remote, and the impact of such concerns, very modest.

### *(m) <u>The rights of the child enshrined in Article 24 of the Charter</u>*

5.7.26 Article 24 of the Charter provides that "*Children shall have the right to such protection and care as is necessary for their well-being. They may express their views freely.*"

5.7.27 Apple notes the reference in Recital 71 of the DSA to the new European strategy for a better internet for kids (BIK+). The three pillars of BIK+ are (1) safe digital experiences to protect children from harmful and illegal content, conduct, contact and risks… and to improve their well-being online; (2) digital empowerment so all children, also those in situations of vulnerability, acquire necessary skills and competences to make sound choices and express themselves in the online environment safely and responsibility; and (3) active participation, respecting them by giving them a say in the digital environment.

5.7.28 The App Store is not a service that is directed at or predominantly used by minors. However, Apple recognises that minors access apps available on the App Store and maintains controls to ensure that they are protected. 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."* Apple notes that a multitude of apps available on the App Store allow parents and guardians to enable their children to learn and acquire new skills to enhance their digital empowerment.

5.7.29 An app store not protected by appropriate risk mitigation measures could give rise to, or be used in a manner giving rise to, risks under this provision. In practice, Apple does enforce the Guidelines to restrict apps or app content which may be harmful to children, and, as detailed in Section 6, maintains a number of controls to protect children. Moreover, as detailed in Section 3, Apple provides parents and guardians with a suite of controls to give them greater choice and oversight of the manner in which their children engage with apps on the App Store.

[36] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.

5.7.30 Were such a Systemic Risk to crystallise, the potential impacts could, again, be severe. Nonetheless, Apple considers that its relevant risk mitigation measures are reasonably and proportionately designed to address this risk. As such, the risk in this area arising from the design or functionality of the App Store must fairly and reasonably be considered to be low.

### *(n) High level of consumer protection, enshrined in Article 38 of the Charter*

5.7.31 Article 38 of the Charter provides that "*Union policies shall ensure a high level of consumer protection.*" As acknowledged in Article 1 of the DSA, Article 38 reflects a requirement on the EU, and not a right having horizontal effect, capable of enforcement as between private persons. Nonetheless, Apple interprets the obligation in Article 34(1)(b) as including a requirement to assess whether the design, functionality or use of the App Store gives rise to any actual or foreseeable negative effects on the provision of a high level of consumer protection to end users of the App Store in the EU. It does not interpret this reference to Article 38 of the Charter in Article 34(1)(b) of the DSA to imply a requirement to assess the App Store's compliance with the consumer protection *acquis* of the EU generally, nor consumer protection laws of each Member State.

5.7.32 The totality of the risk mitigation measures detailed in Section 6 are all designed to ensure that consumers (and indeed developers) are protected when they engage with the App Store.

5.7.33 Absent appropriate controls, the risks of negative effects on consumer protection (across a broad range of potential negative outcomes) would be high, as would be the potential severity of impacts.

5.7.34 Notwithstanding the above, protection of consumers is a foundational principle of the App Store, and the combined effect of the App Store's various risk mitigation measures is to provide end users with a market-leading level of consumer protection.

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

5.8.1 The App Store is a vehicle for the promotion of both private and public civic discourse. Government agencies, non-profits and citizens use the App Store to disseminate apps that contain information and allow them to communicate on matters relating to electoral processes, information relevant to civic discourse and public security.

5.8.2 The purpose and scope of the Systemic Risk referred to in Article 34(1)(c) is not further explained in the recitals to the DSA, although recital (79) contends that VLOPs can be used in "*the shaping of public opinion and discourse*".

### *(a) Electoral processes*

5.8.3 While online platforms can be used to disseminate false information that threatens meaningful debate and electoral processes, and which facilitates the spread of communications antithetical to public security, the likelihood of the App Store being used for such purposes is very substantially lower than for online platforms focussing primarily on UGC. In the App Store, other than apps submitted by malign actors for malign purposes, this would only seem likely to arise in the context of targeted disinformation in ratings and reviews of apps related to civic discourse, electoral processes or public security.

5.8.4 While the potential impacts of such risks crystallising would range from modest to potentially severe, Apple considers its risk mitigation measures to be reasonably and proportionately designed to address this category of Systemic Risk to the extent that it arises from use of the App Store, and to be effective in doing so in practice (as to which, see Section 7 of this Report).

### *(b) Civic discourse and public security (including disinformation)*

5.8.5 As regards potential negative effects on civic discourse and public security, the App Store does not give rise to such risk to an extent remotely comparable with those online platforms whose business models are driven by the widespread dissemination and rapid amplification of content, including UGC or news. The App Store's developer and app approval processes (and its ongoing review of live apps) include controls designed to identify apps intended to have an adverse impact on civic discourse, for example those apps designed to disseminate unlawful extremist content or disinformation.

5.8.6 Recital 84 of the DSA provides that "*When assessing the systemic risks identified in this Regulation, [VLOPs] should also focus on the information which is not illegal, but contributes to the systemic risks identified in this Regulation. [VLOPs] should therefore pay particular attention on how their services are used to disseminate or amplify misleading or deceptive content, including disinformation*".

5.8.7 In practice, Apple does enforce the Guidelines from time to time on grounds capable of having a limiting effect on civic discourse, such as taking action in circumstances where apps include offensive content, or harmful concepts which capitalise or seek to profit on recent or current events, such as violent conflicts, terrorist attacks, or epidemics.

5.8.8 Apple recognises that certain messaging or social media apps that are available on the App Store (and other app stores) have been found to be used to communicate during protests and in times of civil unrest, and that such communications could be seen to adversely impact public security. To the extent that the use of these apps gives rise to public security concerns, such use does not stem from the design, function or use of the App Store. To the extent that users are using an app to disseminate illegal content or incite illegal behaviour, primary responsibility for that content or conduct lies with the user in question, albeit that the developer may have responsibility for the design, function or use of that app.

5.8.9 The risk that user ratings or reviews of apps hosted on the App Store may negatively affect civic discourse, electoral processes, or public security, is low, albeit theoretically possible through co-ordinated disinformation campaigns relating to matters such as public health or security, or to influence elections, or through manipulative behaviour to influence ratings of apps relevant to these matters through use of bots. Apple considers the stringent controls that apply to App Store-hosted UGC proportionate to the risk posed by such content.

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

5.9.1 Recital 83 provides that risks to the protection of public health, minors and serious negative consequences to a person's physical and mental well-being, or on gender-based violence may "stem from coordinated disinformation campaigns related to public health, or from online interface design that may stimulate behavioural addictions of recipients of the service".

### *(a) Gender-based violence*

5.9.2 The risk of actual and foreseeable negative effects stemming from the design, function or use of the App Store relating to gender violence may arise from dissemination in problematic apps or problematic UGC.

5.9.3 The risk of the App Store being used to disseminate apps having a potential adverse effect on gender-based violence is similar to the risks described relating to illegal content under Article 34(1)(a) above.

5.9.4 Similarly, the App Store's controls that protect against illegal and harmful content extend to any app designed to be used in such a way as to have an actual or foreseeable negative effect on gender-based violence.

5.9.5 The probability of exposure to this category of Systemic Risk is similar to that described above for illegal content generally, and were such risks to crystallise, the potential impacts could, again, be severe. Again, however, the App Store maintains risk mitigation measures to address these risks.

5.9.6 In light of the UGC content moderation controls, the risk of user ratings or reviews of apps hosted on the App Store producing negative effects on gender-based violence is low.

### *(b) Protection of minors*

5.9.7 Apple has set out at paragraph 5.7.26 *et seq.* its assessment of the Systemic Risk regarding the rights of the child under Article 24 of the Charter.

### *(c) Protection of public health, serious negative consequences to a person's physical and mental well-being*

5.9.8 Risks to public and individual health do not arise from the use of the App Store in a manner or to an extent remotely comparable with those online platforms whose design, function and / or use involve the widespread dissemination and rapid amplification of UGC. The App Store's developer and app approval processes (and its ongoing review of live apps) include controls designed to identify apps intended to have an adverse impact on public health.

5.9.9 Engagement with the App Store does not give rise to addiction issues that have the potential to cause serious negative consequences to a person's physical and mental well-being. To the extent that such risks arise outside of the App Store after users download apps, Apple's Screen Time functionality, referred to in Section 3, can be used by adults and minors (and their parents) to track and control the time they are spending on particular apps.

5.9.10 The probability of exposure to this category of Systemic Risk arising from the developer use of the App Store, should fairly and reasonably be considered to be no more than modest, although, to the extent that such risk were to crystallise, their impact could be significant. Again, Apple considers its risk mitigation measures to be proportionate and effective in this regard.

5.9.11 In light of the UGC content moderation controls, the risk that user ratings or reviews of apps hosted on the App Store may produce negative effects on public health, physical and mental well-being is low.

### 5.10 Consumer use of apps downloaded from the App Store

5.10.1 This section addresses Apple's approach to Systemic Risks which may arise from consumer use of an app that has been downloaded from the App Store.

5.10.2 As described above, the Systemic Risks may stem from third-party UGC within an app. Those risks do not stem from the design, function or use of the App Store. They stem from the consumer's use of the app. Nor are these risks susceptible to direct control by Apple or by the risk mitigations in place in respect of the App Store; primary responsibility for mitigation of risks arising in connection with such content rests with the developer of the app. If Apple is alerted to UGC engaging Systemic Risks on third-party apps, its practice is to bring such matters to the attention of the app developer so that action can be taken; in the event that appropriate action is not taken, Apple has a range of measures it can take to enforce its requirements on developers under the DSA, but those actions are outside the scope of the DSA, as they stem from the use of third-party apps, not use of the App Store.

5.10.3 Nonetheless, as described below, there are controls in place in respect of the App Store to enable action to be taken to address inappropriate or unlawful UGC in apps published on the App Store.

#### *(a) Mitigation of risks stemming from UGC within a developer's app*

5.10.4 Many online platforms that offer an app on the App Store in the EU are or will be themselves subject to the DSA, in some cases as VLOPs. Those platforms have primary responsibility for the services they offer and any content, including UGC, hosted on their platform. While those platforms are required by Apple to have in place content moderation systems in order to be approved for publication on the App Store, responsibility for moderating UGC on those apps falls to the app developer of the platform, not to the App Store. Nevertheless, apps can and are removed from the App Store if Apple determines that an app does not comply with Section 1.2 of the Guidelines (User-Generated Content).

5.10.5 While concerns around UGC engaging Systemic Risks on such platforms may be brought to the attention of the various teams responsible for the operation of the App Store, Apple is neither required under the DSA, nor in a position to monitor such UGC, and in practice its primary recourse is to bring such UGC to the attention of the developer of the app on which the offending UGC is hosted (see paragraph 5.10.2 above). In the event that the developer fails to act on such a report, Apple may remove the app and / or terminate the developer in accordance with the App Store terms and conditions.

### *(b) Obligations for developers for apps already published on the App Store*

5.10.6 In order for a developer to submit its app to the App Store for distribution, it must comply with the Guidelines. Controls are in place which relate specifically to in-app functionality and content (including specific references to user-generated content), and content moderation. Under the terms of Apple's contractual framework, with which all developers must comply, it is made clear that developers are responsible for complying not only with the Guidelines, but also with all applicable laws.

5.10.7 For example:

(a) The 'Before You Submit' section of the Guidelines makes clear that "*[i]f your app no longer functions as intended or you're no longer actively supporting it, it will be removed from the App Store*". Further, it is clear from Guideline 2.3.1 (Metadata) that developers should not "*include any hidden, dormant, or undocumented features in your app; your app's functionality should be clear to end users and App Review.*" This is echoed by Section 3.3.3 of the DPLA, which provides that "*an Application may not provide, unlock or enable additional features or functionality through distribution mechanisms other than the App Store, Custom App Distribution or TestFlight*".

(b) As regards app content, the Guidelines stipulate that "*Apps should not include content that is offensive, insensitive, upsetting, intended to disgust, in exceptionally poor taste, or just plain creepy*" (Guideline 1.1 (Objectionable Content)). Examples given in the Guidelines of objectionable content include defamatory, discriminatory, or mean-spirited content; realistic portrayals of violence including people or animals being killed, maimed, tortured, or abused; overtly sexual or pornographic material; and harmful concepts which capitalise or seek to profit on recent or current events.

(c) Developers must also take steps to enable moderation of an app's user-generated content, in particular those apps which contain user-generated content. Guideline 1.2 (User-Generated Content) provides that apps which include user-generated content must include tools to prevent abuse, including a method for filtering objectionable material from being posted to the app, a mechanism to report offensive content and timely responses to concerns, the ability to block abusive users from the service, and published contact information so users can easily reach the relevant developer.

## 5.11 Risks if Apple's key mitigation measures do not fully address the Systemic Risks

5.11.1 For the reasons set out above, although Apple considers that each of the Systemic Risks described above could stem from the design, function or use of the App Store, they are all risks that Apple recognises and mitigates. And, as described in Section 6 below, Apple's risk mitigation measures are continually adapted and improved to build on learning and address ever-evolving risks.

5.11.2 As with any controls framework, there is always a measure of risk arising from the fact that the existing risk mitigation measures in place cannot be expected to have a 100% success rate to mitigate the Systemic Risks which may stem from the App Store, particularly as the nature of threats evolve. These may include, for example:

(a) the risk that the App Store's terms and conditions do not fully address the Systemic Risks or afford Apple a basis for enforcing them in order to mitigate Systemic Risks;

(b) the risk that the developer onboarding process fails to identify a developer whose intent to is publish apps which may give rise to Systemic Risks;

(c) the risk that the automated review systems of the App Review process fail to detect illicit app binary functionality;

(d) the risk that the App Store human app review does not identify apps that do not comply with the terms and conditions, in particular the Guidelines;

(e) the risk that recommender and algorithmic systems deployed in connection with the App Store recommend and display apps that are illegal in specific regions or have adverse impacts in respect of the other Systemic Risks;

(f) the risk that the App Store systems that moderate UGC on the App Store (that is to say app ratings and reviews) do not detect and remove UGC engaging the Systemic Risks; and

(g) the risk that the App Store notice and action systems do not adequately provide a means for Apple employees, or developers, users or third parties to raise alerts regarding apps or UGC engaging Systemic Risks.

5.11.3 These matters are among those considered in addressing the reasonableness, proportionality and effectiveness of Apple's App Store risk mitigation measures in Section 7.

## SECTION 6: MITIGATION OF POTENTIAL SYSTEMIC RISKS ARISING FROM THE DESIGN, FUNCTIONING OR USE OF THE APP STORE

### 6.1 Section overview

6.1.1 Section 3 of this Risk Assessment provides details regarding relevant Apple ecosystem functions, policies and protections. These are not repeated here.

6.1.2 Section 4 of this Risk Assessment provides an overview of the way users can discover and download apps from the App Store, as well as a high-level description of key controls that apply before an app is published. Section 5 of this Risk Assessment then identifies the way in which Systemic Risks might potentially crystallise in the App Store.

6.1.3 This Section provides more detail on key control functions and the risk mitigation measures that form part of the design or functioning of the App Store that operate to keep the App Store a safe and trusted place for all users. Apple considers that the risk mitigation measures detailed in this Section and elsewhere in the report constitute risk mitigation measures relevant to its obligation under Article 35 of the DSA to put in place reasonable, proportionate and effective risk mitigation measures.

6.1.4 The Section is structured as follows:

(a) App Store Policies, Terms and Conditions that mitigate systemic risks;

(b) Developer Due Diligence Measures;

(c) App Review;

(d) App Store and Privacy;

(e) Recommender Systems Risk Mitigation Measures;

(f) App Store User-Generated Content Measures;

(g) App Store External Notice and Action Measures; and

(h) New DSA Compliance function.

### 6.2 App Store Policies, Terms and Conditions that mitigate systemic risks

6.2.1 Pursuant to Article 34(2) of the DSA, Apple is required to assess how certain listed factors influence the Systemic Risks. These factors include "the applicable terms and conditions and their enforcement". An overview of App Store terms and conditions and their enforcement is detailed below.

#### *(a) App Store consumer terms and conditions*

6.2.2 Before an end user can use the App Store, they must agree to the Apple Media Service Terms and Conditions (the "AMS Terms"),[37] which govern the use by end users of the App Store service.

[37] https://www.apple.com/legal/internet-services/itunes/ie/terms.html

6.2.3 Use of the App Store requires the creation of an Apple ID. Anyone 13 years of age or over, or the equivalent minimum age in their country or territory of residence, can create an Apple ID.[38] Apple IDs for individuals under this age can be created by parents or guardians using Family Sharing.[39] Apple recommends that parents or legal guardians creating an account for a minor should review the AMS Terms with the minor to ensure they understand it.

6.2.4 The AMS Terms contain Submission Guidelines that apply to user ratings and reviews on the App Store. The Guidelines prohibit various forms of misuse, including using the App Store to:

(a) post any materials that (i) users do not have permission, right or licence to use, or (ii) infringe on the rights of any third party;

(b) post objectionable, offensive, unlawful, deceptive, inaccurate or harmful content;

(c) post personal, private or confidential information belonging to others;

(d) request personal information from a minor;

(e) post, modify or remove a rating or review in exchange for any kind of compensation or incentive;

(f) 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

(g) plan or engage in any illegal, fraudulent, or manipulative activity.

6.2.5 In addition, the AMS Terms detail various prohibitions including: manipulating play counts, downloads, ratings or reviews via any means, including the use of bots, scripts, or automated processes, or providing or accepting any kind of compensation or incentive. Users who breach these requirements can be removed from the App Store.

6.2.6 The AMS Terms also explain that users can report use of the App Store that does not comply with the Submission Guidelines via the "Report a Concern" function.

6.2.7 The AMS Terms also set out the requirements for "Family Sharing" accounts. The "family organizer" must be 18 (or an equivalent age of majority in their country or

[38] When a user creates an Apple ID they are asked for their date of birth. If a user is below the relevant age, then a parent must create the Apple ID. As part of the process of creating an Apple ID for a child, parents will be asked to provide information required to create an account which may include: the child's full name, date of birth, a password and a phone number. Where a parent is creating an account for a child under the age of 13, Apple may require that the parent confirm a payment method Apple already maintains for the parent. Beyond that, and in keeping with Apple's approach to privacy, the principles of the UK Information Commissioner's Office Children's Code, and Article 28(3) of the DSA, Apple collects as little information about children as possible. To that end, Apple does not request proof of age and does not analyse biometrics or use other technologies to assess age.

[39] See paragraph 3.4.2 *et seq*.

territory of residence), and the parent or legal guardian of any users under age 13. The AMS Terms also explain how purchase sharing works, and the ways in which eligible content is shared among members of a family, including the "Ask to Buy" feature.

6.2.8 The AMS Terms also make clear that the developer of any third-party app is solely responsible for its content, subject to local law.

6.2.9 The AMS Terms explain to users the factors that determine how results are presented when they use the App Store search function, including metadata provided by the app developer, user engagement with apps and the App Store, and an apps' popularity.

6.2.10 Finally, the AMS Terms also explain to users how they can contact Apple if they believe that content featured on the App Store infringes their copyright, with a separate link and notice associated with third-party apps.[40] They also explain the steps Apple can take against a user who is found to have repeatedly infringed the copyrights of others. The AMS Terms refer to redress options available to users who have been notified that their reviews have been removed from the App Store.

### *(b) App Store developer terms and conditions*

#### (i) Apple Developer Agreement

6.2.11 To get access to certain resources for learning how to develop apps, developers must execute the ADA.[41] The ADA contains the terms and conditions for registering with Apple to become an Apple Developer and governs the use of the Apple Developer website, beta software and events, and may include the opportunity to attend certain Apple-provided technical talks and other events, including online or electronic broadcasts of such events. It also addresses export controls, including prohibitions against contracting with sanctioned individuals and entities.

6.2.12 If a developer breaches the terms of the ADA, Apple can at its discretion terminate or suspend the developer.

#### (ii) Apple Developer Program License Agreement

6.2.13 To enrol in the Apple Developer Program (a necessary step for developers wishing to publish apps on the App Store), developers must also execute the DPLA, enrolling as an individual or an organisation (e.g., company, non-profit, government organisation).[42] An individual or an authorised employee of an organisation must use an Apple device (while being logged into iCloud and using their Apple ID with two-factor authentication turned on) to log into the Apple Developer website or app, where they review and accept the DPLA. If they are logged into the Apple Developer

[40] https://www.apple.com/legal/internet-services/itunes/appstorenotices/#?lang=en

[41] https://developer.apple.com/support/downloads/terms/apple-developer-agreement/Apple-Developer-Agreement-20230605-English.pdf

[42] https://developer.apple.com/programs/apple-developer-program-license-agreement/

app, they must also verify their identity using a government-issued photo ID. Organisations must provide information about the organisation (for example, entity type; legal entity name; D-U-N-S Number; headquarters address and phone number; website; and signing authority confirmation).

6.2.14 The DPLA grants a limited licence to developers to use certain Apple software and services for app development; apps may be distributed through the App Store, or through other distribution channels (for example, Custom App Distribution to organisational customers, ad hoc testing on registered devices, TestFlight for beta testing). Below is a summary of some relevant provisions:

6.2.15 Section 3.2 provides that developers will not use the Apple software or services, including the App Store, to:

(a) engage in unlawful or illegal activity, nor to develop products which would commit or facilitate the commission of a crime, or other tortious, unlawful or illegal acts;

(b) threaten, incite or promote violence, terrorism or other serious harm;

(c) create or distribute any content or activity that promotes child sexual exploitation or abuse;

(d) violate, misappropriate or infringe proprietary or legal rights;

(e) violate the security, integrity or availability of any user, network, computer or communications system; or

(f) engage, or encourage others to engage, in any unlawful, unfair, misleading, fraudulent, improper or dishonest acts or business practices (for example, engaging in bait-and-switch pricing, consumer misrepresentation, deceptive business practices, or unfair competition against other developers).

6.2.16 Section 3.3 provides that developers must, in the app description on the App Store, provide clear and complete information to users regarding their collection, use and disclosure of user or device data. They are also required to take appropriate steps to protect such data from unauthorised use, disclosure or access by third parties. In addition, developers must maintain a privacy policy, which details their collection, use, disclosure, sharing, retention, and deletion of user or device data, and must be published on its website with a link in the App Store.

6.2.17 Section 11.2 explains that Apple can terminate a DPLA with a given developer if the developer:

(a) violates the DPLA, including the terms listed above in Section 3.2;

(b) becomes subject to sanctions or other restrictions in relevant regions; or

(c) engages, or encourages others to engage, in any misleading, fraudulent, improper, unlawful or dishonest act, including misrepresenting the nature of an app (for example, hiding or trying to hide functionality from Apple’s review, falsifying consumer reviews, or engaging in payment fraud).

### (iii) Schedules 1 and 2 to the DPLA

6.2.18 To distribute apps through the App Store, Apple Developers must accept the terms of Schedule 1 (for free apps) or Schedule 2 (paid apps or apps using Apple's In-App Purchase API) to the DPLA.[43] These Schedules appoint ADI as the commissionaire for the marketing and end user download of apps distributed in the EU. The Schedules also contain requirements for the delivery of apps to Apple and end users; ownership of apps and app information; end user licensing; content restrictions; and age ratings. In addition, Schedule 2 addresses commerce and tax issues. Below is a summary of some relevant provisions:

6.2.19 Section 2.4 provides that the developer is responsible for:

(a) 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; and

(b) providing any content restriction tools or age verification functionality before enabling end users to access mature or otherwise regulated content within their app.

6.2.20 Section 5 requires developers to warrant and represent that:

(a) their app does not (or permit users to) violate intellectual property or contractual rights;

(b) their app is authorised for distribution, sale and use in, export to, and import into each of the regions designated;

(c) their app does not contain any obscene, offensive or other materials prohibited or restricted under the laws or regulations of any of the regions they designate for distribution;

(d) their app information is accurate;

(e) they will provide correct and complete information about the content of their app in assigning an app rating;

(f) their app shall not target children in any region where doing so is illegal; and

(g) their app complies with all applicable laws where distributed, including consumer protection, marketing, and gaming laws.

6.2.21 Section 7.3 explains that Apple may cease the marketing and allowing download of an app (for example, remove an app or terminate a developer) if the developer or app:

(a) is not authorised for export;

(b) infringes intellectual property rights;

[43] https://developer.apple.com/support/downloads/terms/schedules/Schedule-2-and-3-20220225-English.pdf

(c) violates any applicable law;

(d) violates the terms of the DPLA, Schedules to the DPLA, or the Guidelines; or

(e) is subject to sanctions of any region in which Apple operates.

6.2.22 Revisions to the DPLA Schedules make reference to redress options available to developers who have been notified that that their app has been removed from the App Store or that their developer account has been terminated.

6.2.23 As reported in Apple's 2022 Transparency Report, Apple terminated 428,487 developer accounts, the vast majority of which were due to non-compliance with Section 3.2(f) of the DPLA (which prohibits developers using Apple's services to engage, or encourage others to engage, in any unlawful, unfair, misleading, fraudulent, improper, or dishonest acts or business practices, including bait-and-switch pricing, consumer misrepresentation, deceptive business practices, or unfair competition against other developers). Only 3,338 of those were appealed, and of those only 159 resulted in account restorations.[44]

### (iv) App Store Review Guidelines

6.2.24 All Apple Developers who want to distribute apps in the App Store must comply with the Guidelines, which provide requirements for apps to be approved and remain available on the App Store.[45] The five pillars of the Guidelines are Safety (Section 1), Performance (Section 2), Business (Section 3), Design (Section 4), and Legal (Section 5). Overall, the Guidelines require that apps offered on the App Store are safe, provide a good user experience, adhere to Apple's rules on user privacy, secure devices from malware and threats, and use approved business models.

6.2.25 All new apps and updates to existing apps are reviewed for compliance with the Guidelines. Specific provisions of the Guidelines are discussed in more detail below in the section addressing App Review risk mitigation measures.

6.2.26 The Guidelines are subject to periodic review, updates, and additions, to account for the needs of customers, developer innovation, changes in technology and law, ongoing App Review learnings, and developments in the App Store risk landscape. This offers opportunities to enhance the Guidelines and address risk generally, including the Systemic Risks. For example, Guideline 1.1.7, which prohibits harmful concepts which seek to profit from current events, including violent conflict, terrorist attacks and epidemics, was put in place [CONFIDENTIAL].[46] While Apple strives for continuity in the Guidelines, changes in developer practices, technology and risk as well as the desire to provide transparency to developers require periodic updates of the Guidelines to be made.

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

[45] https://developer.apple.com/app-store/review/guidelines/

[46] https://developer.apple.com/news/?id=xk8d7p8c

6.2.27 The App Store provides mechanisms for developers to submit feedback on the Guidelines via the "suggest a guideline" form, and such feedback is factored in when the Guidelines are under review.[47] The App Review team compiles requests and suggestions on modifications to the Guidelines, [CONFIDENTIAL]. Changes to the Guidelines have occurred annually, and sometimes multiple times a year. Once an update is made, the reviewed Guidelines are published online and developers are notified of the update, both via email and a dedicated update published on Apple's "News and Updates" area of the Apple Developer web site.

## 6.3 Developer Due Diligence Measures

### *(a) Sanctions screening*

6.3.1 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.

6.3.2 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.

6.3.3 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.

### *(b) Identity verification and screening*

6.3.4 As explained above, individuals and organisations must sign in with an Apple ID with two-factor authentication, review and accept the latest terms of the Apple Developer Agreement,[48] 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.

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

[47] https://developer.apple.com/app-store/review - see "Suggestions".

[48] https://developer.apple.com/support/downloads/terms/apple-developer-agreement/Apple-Developer-Agreement-20230605-English.pdf

6.3.6 The enrolment screening process helps Apple identify and therefore stop fraudulent or sanctioned actors whom Apple determines to be likely to develop and distribute apps that may contain illegal or harmful content from gaining access to the App Store.

## 6.4 App Review

6.4.1 Apps and app updates submitted to the App Store are uploaded through App Store Connect, where developers create an app record, provide app metadata (including app binary), 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). All such data relating to apps and app updates are then reviewed by both automated tools and human app review specialists, both of which are a critical component of App Review.

6.4.2 There are more than 100,000 app submissions in an average week. In 2022, App Review reviewed 6,101,913 submissions (including app updates). The App Review team rejected over 25 % of those submissions for various compliance issues, thereby serving an important function in mitigating risks, including potential Systemic Risks, in the App Store.[49]

### *(a) <u>Automated review</u>*

6.4.3 Upon receipt of an app or app update, the App Review automated review process conducts a static binary analysis, asset analysis, and runtime analysis [CONFIDENTIAL] and analyse threats and signals (for example, the presence of malicious URLs or executable code, which for example could introduce or change features or functionality of the app). The automated review process also conducts checks [CONFIDENTIAL], and cross-references apps and developers against previously identified threats in the App Store ecosystem to better detect malicious actors, fraud, and other abuses.

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

[49] https://www.apple.com/legal/more-resources/docs/2022-App-Store-Transparency-Report.pdf. *See also* the supplemental data file at https://www.apple.com/legal/zip/2022-Supplemental-Data-File.zip.

[50] [CONFIDENTIAL].

6.4.5 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.

6.4.6 The information gathered during automated review flags potential risks and provides useful signals and information to human app reviewers to evaluate in more detail. In addition, such information is used to train the machine learning algorithms to continually improve detection and rejection of problematic apps. Finally, as explained in more detail below, automated processes continue after approval of apps that are available on the App Store, with automated detection and escalation mechanisms continuing to scan for potential threats.

6.4.7 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.

### *(b) Human review*

6.4.8 The human review component of App Review is critical to the App Store's mitigation and management of Systemic Risks. Every app and every app update undergoes human review, where trained app review specialists evaluate app features and functionality and signals provided by automated systems to screen out deceptive and abusive behaviour and ensure compliance with the Guidelines.

6.4.9 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, while the automated review will identify data access entitlements and API calls, a human app reviewer is trained to assess whether use of the entitlements and APIs are appropriate for the app's functionality. For example, a human app reviewer will likely decide that a calculator app does not need to request access to data and functionality like photos or the microphone. Similarly, app reviewers are trained to evaluate whether an app age rating is appropriate given the app's content and functionality, as well as whether apps with user-generated content have sufficient content moderation mechanisms to protect children or mitigate risks related to offensive content, harmful concepts, or public security.

6.4.10 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.

6.4.11 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.

6.4.12 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.

6.4.13 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.

6.4.14 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 in paragraph 6.4.13 above.

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

### *(c) General review practices*

#### (i) App Review Guidelines

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

6.4.17 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.

6.4.18 Particularly relevant to the DSA are Guidelines that:

(a) Prohibit objectionable content;

(b) Contain specific rules for apps with UGC;

(c) Contain specific rules for apps in the Kids category;

(d) Require developers to set appropriate age ratings; and

(e) Require compliance with privacy, intellectual property, consumer protection and all other applicable laws, including the U.S. Federal Children's Online Privacy Protection Rule ("COPPA") and GDPR.

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

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

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

6.4.21 In 2022, 92,598 apps were rejected for non-compliance with Section 1 of the Guidelines.[51]

#### (A) Objectionable content

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

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

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

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

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

(e) harmful concepts which capitalise on current events.

#### (B) User-generated content

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

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

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

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

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

(d) published developer contact information.

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

(C) Kids category[52]

6.4.25 Section 1.3 (Kids category) provides that apps in the "Kids" category must not include links out of the app, purchasing opportunities, or other distractions to kids unless reserved for a designated area behind a "parental gate".[53] In addition to complying with privacy laws applicable to children, Kids Category apps may not send personally identifiable information or device information to third parties and should not include third-party analytics or third-party advertising. In limited cases, third-party analytics may be permitted provided that the services do not collect or transmit any identifiable information about children (such as name, date of birth, email address), their location, or their devices. Any third-party contextual advertising services in Kids category apps must have publicly documented practices and policies for Kids Category apps that include human review of ad content for age appropriateness (and a link must be provided to such policies and practices when the app is submitted for App Review).

(D) Physical harm

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

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

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

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

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

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

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

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

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

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

6.4.29 Section 5 of the Guidelines states that apps must comply with all legal requirements in any location where developers make them available, and specifies that the developer is responsible for understanding and ensuring their app conforms with all local laws. In addition, Section 5 states apps that solicit, promote, or encourage criminal or clearly reckless behaviour are unacceptable, and warns that in extreme cases, such as apps that are found to facilitate human trafficking and / or the exploitation of children, the appropriate authorities will be notified.

6.4.30 In 2022, 441,972 apps / app updates were rejected for non-compliance with Section 5 of the Guidelines.

(A) Privacy

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

(B) Data practices

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

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

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

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

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

(e) respect user permission settings;

(f) allow app use without a login if the app doesn't rely on account-based features; and

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

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

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

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

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

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

(C) Health

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

(D) Kids

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

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

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

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

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

(E) Location services

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

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

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

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

(F) Intellectual property

6.4.37 Section 5.2 (Intellectual Property) requires developers to only include content in their app if they own it or are licensed or otherwise have permission to use it, and directs developers who believe that their intellectual property rights have been infringed by another developer on the App Store to submit a claim via the App Store Content Dispute web form. [54] If the app features third-party trademarks or copyrighted content or lets users stream or download third-party content, the developer must provide with its app submission its authorisation to use such content.[55]

(G) Gaming, Gambling and Lotteries

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

[54] https://www.apple.com/legal/internet-services/itunes/appstorenotices/#?lang=en

[55] https://developer.apple.com/app-store/review/

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

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

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

(d) must be free on the App Store.

(H) Developer Code of Conduct

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

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

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

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

### *(d) App review escalations and new and emerging issues*

6.4.40 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] new technologies [CONFIDENTIAL]. Below are the key groups involved in app escalations.

#### (i) App Review Compliance

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

### (ii) App Store Improvements/Technical Investigations

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

### (iii) App Review Policy

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

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

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

### (v) ERB

6.4.45 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.

6.4.46 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.

### *(e) <u>App review rejections, suspensions, terminations, appeals</u>*

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

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

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

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

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

6.4.52 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").[56] 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.

6.4.53 Very few appeals are sustained, which tends to confirm the robust nature of app removal and developer termination decisions. For example, in 2022, Apple removed 186,195 apps from the App Store. Only 18,412 of those decisions were appealed, and 616 resulted in the app being restored.[57] Similarly, 428,487 developer accounts were terminated. Only 3,338 developer account terminations were appealed and, of those, 159 resulted in a restoration.[58]

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

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

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

### *(f) Ongoing monitoring*

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

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

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

(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.

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

## 6.5 App Store and Privacy

6.5.1 Pursuant to Article 34(2) of the DSA, Apple is required to assess how its "*data related practices*" influence the Systemic Risks. An overview of relevant practices and controls is detailed below.

### *(a) App Store & Privacy Notice*

6.5.2 When first interacting with the App Store, users are presented with service-specific privacy information, in the form of the App Store & Privacy Notice.[59] This ensures that users have an effective choice and any consent to data use on Apple products is fully informed.

6.5.3 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.

[59] https://www.apple.com/legal/privacy/data/en/app-store/

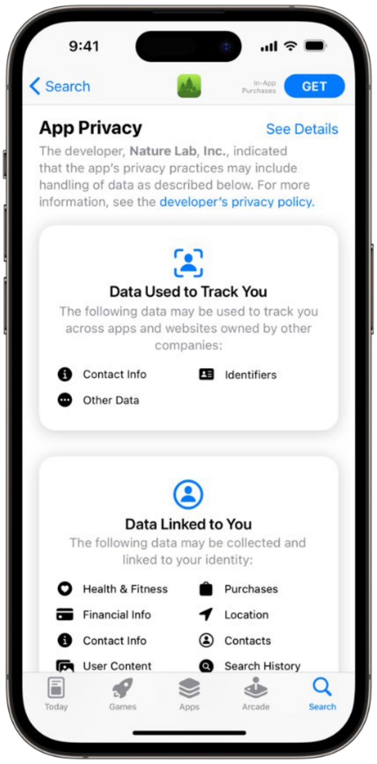
6.5.4 The App Store uses, inter alia, local, on-device processing to enhance its recommendations and mitigate privacy risks. In addition, using data such as app installs – the App Store can suggest apps and in-app events that are more relevant to users. These recommendation systems are described from paragraph 6.6 below.

6.5.5 The App Store & Privacy Notice also explains how users can turn off personalisation features. Personalisation is also described in further detail from paragraph 6.6.32 below.

6.5.6 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.

### *(b) <u>Privacy Nutrition Labels</u>*

6.5.7 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.



**App Privacy** See Details

The developer, **Nature Lab, Inc.**, indicated that the app's privacy practices may include handling of data as described below. For more information, see the developer's privacy policy.

**Data Used to Track You**

The following data may be used to track you across apps and websites owned by other companies:

- Contact Info
- Identifiers
- Other Data

**Data Linked to You**

The following data may be collected and linked to your identity:

- Health & Fitness
- Purchases
- Financial Info
- Location
- Contact Info
- Contacts
- User Content
- Search History

6.5.8 The same applies to Apple's own apps.[60] 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.

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

### *(c) App Privacy Report*

6.5.9 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.[61] Via this report, users are able to see how often their location, photos, camera, microphone, and contacts have been accessed by apps during the last seven days, and which domains those apps have contacted. Users therefore have full and easy visibility into the ways apps use the privacy permissions a user has granted them, as well as their respective network activity. Together with Privacy Nutrition Labels, this feature provides users with transparent information about how the apps made available on the App Store treat user privacy.

### *(d) App Tracking Transparency Framework*

6.5.10 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. If the user has not granted permission to this tracking, the relevant app will not be able to access any user data.

6.5.11 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.

### *(e) Access Permissions and App Sandbox*

6.5.12 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.

[61] https://support.apple.com/en-us/HT212958

6.5.13 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.

## 6.6 Recommender Systems Risk Mitigation Measures

6.6.1 Pursuant to Article 34(2) of the DSA, Apple is required to assess how its "*recommender systems and any other relevant algorithmic systems*" influence the Systemic Risks. An overview of App Store recommender systems, and the search function is detailed below.

6.6.2 As explained in Section 4 above, users can discover apps available in the App Store through five tabs: Today, Games, Apps, Arcade, and Search. The apps that are displayed in these tabs appear organically (for example, various categories of "Top" charts ) in all tabs except Search; as "recommendations" in the form of algorithmically selected recommendations or editorially curated recommendations in all tabs; as a search result in the Search tab; or as an Apple Search Ad in the Today or Search tabs. App recommendations may also be personalised based on a user's demographic, as well as App Store purchase and download history. Notably, all apps appearing in the App Store, including recommendations, have already undergone the rigour of the App Review process and have been approved for publication in the App Store.

### *(a) Algorithmically Selected App Recommendations*

6.6.3 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].

6.6.4 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.

6.6.5 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].

### *(b) Editorially Curated App Recommendations*

6.6.6 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.

6.6.7 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.

6.6.8 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.

6.6.9 The Editorial team maintains and updates curation guidelines, which identify apps that are "not recommendable" (despite having been through App Review) and local sensitivities, for editors to reference. 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.[62]

### *(c) App Store Search Results function*

6.6.10 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.

6.6.11 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.

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

6.6.12 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.

6.6.13 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.

6.6.14 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.

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

6.6.16 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.

### *(d) <u>Apple Search Ads</u>*

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

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

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

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

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

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

6.6.23 Apple takes several measures to address risk relating to Apple-delivered promoted app placement on the App Store. For example, in addition to the actions performed by the App Review team to review and approve apps for distribution on the App Store, the Apple Search Ads team additionally reviews promoted app placement for content, imagery, and promotion category classification. Apple Search Ads policies prohibit certain categories of apps from being promoted on the App Store – either altogether, in certain countries or regions, or in certain App Store placements.[63] Moreover, some categories of apps that are not prohibited may still face promotion restrictions as managed by the Apple Search Ads team – for example, submitting proof of specific permits or licences to Apple as a prerequisite to advertising, including the promotion of apps, in certain countries or regions.

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

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

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

6.6.27 Information to assign a user to segments is strictly limited and includes account information (for example, name, address, age, gender), downloads, purchases and subscriptions records on the App Store. When selecting which Apple Search Ad to display from multiple ads for which a user is eligible, Apple may use some of this information, as well as App Store searches and browsing activity, to determine which

[63] https://searchads.apple.com/policies/

ad is likely to be most relevant. This information is aggregated across users so that it does not identify any single user.

6.6.28 Pursuant to its obligation under Article 39 of the DSA, Apple has created a public online repository of apps promoted as Apple Search Ads.[64] The repository sets out information about each app presented as an Apple Search Ad to consumers within the EU, including what content was presented where, and when. The repository is designed to contain this information for the period that the Apple Search Ad unit is live, and for one year from the date of its last impression. For content that is restricted due to alleged illegality, a governmental order, or incompatibility with applicable terms and conditions, the repository is designed to record the restriction as well as the grounds for the restriction. The repository is accessible and can be queried through a dedicated website. An API is also available for large volume queries.

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

(a) For a minor under 18 (or the age of majority in the relevant jurisdiction) who is logged in with their Apple ID, the Personalised Ads setting is automatically set to "off" and cannot be enabled until the user reaches the age of majority. With Personalised Ads set to off, Apple cannot use account information (for example, name, address, age, gender), apps downloads, or in-app purchases and subscriptions, for serving Apple Search Apple Search Ads in the App Store.

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

6.6.30 Furthermore, as explained in Section 4 above, each app has an age rating. These age ratings, and the age of the user, determine whether, and if so, which Apple Search Ads will be displayed to users under 18 years of age, subject always to the following limitations:

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

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

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

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

### *(e) <u>Personalisation</u>*

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

[64] https://adrepository.apple.com/

6.6.33 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.

6.6.34 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).

6.6.35 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.

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

6.6.37 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.

### *(f) Mitigating potential third-party abuses*

6.6.38 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.

6.6.39 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 supressing 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.

6.6.40 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.

## 6.7 App Store User-Generated Content Measures

6.7.1 Pursuant to Article 34(2) of the DSA, Apple is required to assess how its "content moderation systems" influence the Systemic Risks. The App Review process is detailed earlier in this Section. An overview of App Store UGC controls is detailed below.

6.7.2 As explained above, the only UGC on the App Store is user-generated app ratings and reviews.

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

6.7.4 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.

6.7.5 A number of monitoring processes are carried out to protect against fake or fraudulent reviews, and developer responses, including scanning for spam, profanity and foul language, and multiple duplicate or similar entries.

6.7.6 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.

6.7.7 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 from paragraph 6.8.9 below.

6.7.8 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.

6.7.9 In 2022, App Store processed over one billion ratings and reviews, of which more than 147 million were blocked and removed for failing to meet its moderation standards.[65]

## 6.8 App Store External Notice and Action Measures

6.8.1 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

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

in place that ensure that only a smaller subset of apps are recommended to users, either as recommended or editorial content, or as Apple Search Ads.

6.8.2 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.

### *(a) <u>Report a Problem</u>*

6.8.3 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.

6.8.4 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.

6.8.5 [CONFIDENTIAL].

6.8.6 [CONFIDENTIAL].

6.8.7 [CONFIDENTIAL].

6.8.8 [CONFIDENTIAL].

### *(b) Report a Concern*

6.8.9 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.

6.8.10 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".

6.8.11 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 post offensive, illegal, or misleading responses to critical reviews.

(c) Developers are encouraged in the event they see a review of 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.

6.8.12 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.

6.8.13 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.

6.8.14 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.

### (c) *Notices Routed to App Store Legal*

6.8.15 The App Store Legal team is responsible for reviewing and vetting notices from external sources that involve issues with apps in the App Store. Government regulatory authorities routinely send notices to the App Store via a dedicated email inbox, [CONFIDENTIAL]. Such notices typically involve a request for information about an app or developer, or demand to take down an app pursuant to local law or court order. Likewise, local law enforcement authorities send notices and requests for information to a similar dedicated email inbox, lawenforcement@apple.com. 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.

6.8.16 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.

### *(d) Content disputes*

6.8.17 Rights holders can submit App Store content disputes via a dedicated webpage.[66] These submissions are routed to the AMS Content Disputes Legal team for consideration.

6.8.18 Once the AMS Content Disputes Legal team receives a complete complaint, the team responds with a reference number.[67] 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.

6.8.19 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.

6.8.20 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.

6.8.21 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.

### *(e) New Content Reports portal for DSA*

6.8.22 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.

6.8.23 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

[66] https://www.apple.com/legal/internet-services/itunes/appstorenotices/#/contacts?lang=en

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

goes through the process flow outlined from paragraph 6.8.3 *et seq.* above. If they select the latter, they are redirected to the Content Reports portal.

6.8.24 [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.

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

6.8.26 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.

6.8.27 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.

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

## 6.9 New DSA Compliance function

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

6.9.2 On 24 August 2023, the ADI Board formally appointed the Head of DSA Compliance. The individual in question is an experienced compliance professional, with extensive compliance experience, who has the required professional qualifications, knowledge and ability to fulfil the role. The individual in question has an in-depth knowledge of Apple's products and services and has for many years been responsible for internal and external risk management and risk mitigation strategies, including across the EU.

6.9.3 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.

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

(a) cooperating with the Digital Services Coordinator to be designated by Ireland 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.

6.9.5 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.

### 6.10 New DSA Information site

6.10.1 Apple has created a new DSA information site - https://www.apple.com/legal/dsa/, 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 new Content Reports portal;

(c) a link to the new Ads Repository;

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

(e) a link to the average monthly recipients report.

6.10.2 Additional resources, for example transparency reports, will be added to the site in due course.

## SECTION 7: REASONABLENESS, PROPORTIONALITY AND EFFECTIVENESS OF APP STORE RISK-MITIGATION MEASURES

### 7.1 Section overview

7.1.1 Pursuant to Article 35 of the DSA, Apple is required to implement "reasonable, proportionate and effective mitigation measures tailored to the specific systemic risks identified pursuant to Article 34, with particular consideration to the impacts of such measures on fundamental rights".

7.1.2 This Section of the Report sets out why Apple considers that the existing risk mitigation measures detailed in this Report, as supplemented by the new risk mitigation measures Apple has implemented, or will be required to implement, in order to comply with the DSA, are reasonable, proportionate and effective to address the Systemic Risks described in Section 5 that could stem from the design, function or use of the App Store.

### 7.2 The App Store and its approach to risk mitigation

7.2.1 The App Store's risk mitigation measures have been developed with the benefit of the experience of inventing and establishing the wholly novel business model underlying the App Store, and the subsequent 15 years' experience of operating the App Store, dealing throughout that period with issues engaging or potentially engaging manifold risks, including the Systemic Risks, and developing and continuously improving the controls environment applicable to the App Store.

7.2.2 Apple notes Recital 79 of the DSA states that "*[VLOPs…] can be used in a way that strongly influences safety online, the shaping of public opinion and discourse, as well as online trade. The way they design their services is generally optimised to benefit their often advertising-driven business models and can cause societal concerns*." While Apple agrees that trust and safety are key considerations for the App Store, it is clearly not the case that the App Store is optimised to benefit an advertising-driven business model.

7.2.3 The success of the App Store has been built upon end users' trust that all apps available on the App Store respect the high standards of security, privacy, performance, user safety and product integrity to which Apple is committed. This benefits end users, who rely on the App Store as a trusted place where they can download apps that have been subject to both automated and human review. It also benefits developers, who rely on it as a way to connect to potential customers across the EU and around the world.

7.2.4 It is widely recognised that Apple effectively manages risks relating to the App Store. This success is demonstrated by the significant number of apps and developers which Apple keeps out of the App Store each year, compared to the relatively few occurrences of problematic apps being in the App Store and the swiftness with which any such examples are addressed.

7.2.5 The experience to date therefore points to Apple having struck a reasonable balance in maintaining a safe, predictable and trusted online environment, while at the same time recognising and effectively mitigating relevant risks, including protecting fundamental rights. Nonetheless, Apple's guiding principle for the App Store – to provide a safe and trusted place for customers to discover and download apps – is wholly aligned with the legislative purposes underpinning the DSA.

7.2.6 Apple is conscious that no compliance framework – nor any individual risk mitigation measure – operates with a 100% success rate. The hallmark of an effective compliance framework is that it earnestly and efficaciously addresses known risks, and evolves and adapts promptly to address new and emerging risks. That is undoubtedly the case with the App Store risk mitigation framework. As has been the case throughout the existence of the App Store, Apple will continue to keep the ongoing effectiveness of the App Store controls and risk mitigation measures under continuous review to address the evolving risk environment the App Store faces.

### 7.3 Reasonableness, proportionality and effectiveness of App Store risk-mitigation measures

7.3.1 None of the terms "*reasonableness*", "*proportionality*" or "*effectiveness*" are defined in the DSA; nor is there an equivalent regime to Articles 34 and 35 of the DSA to be found elsewhere in the *acquis communautaire*.

7.3.2 The risk mitigation measures in place and required in connection with the App Store can be considered on the basis of the ordinary, natural meaning of these words. Nonetheless, with a view to benchmarking those measures against comparable existing standards, Apple has considered the use of these words (or the use of analogous standards) in leading governmental guidance in jurisdictions outside the EU relating to the evaluation of corporate compliance structures, including the U.S. Department of Justice Guidance for Prosecutors – "*Evaluation of Corporate Compliance Programs*" (Updated March 2023) (the "US DOJ Guidance"), the U.K. Ministry of Justice *Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing (section 9 of the Bribery Act 2010)* (the "UK MoJ Guidance") and the UK HM Revenue & Customs guidance of September 2017 *Tackling tax evasion: Government guidance for the corporate offences of failure to prevent the criminal facilitation of tax evasion* (the "UK HMRC Guidance"), and within the EU, in the form of the French Anti-Corruption Agency Guidelines of January 2021 on the compliance arrangements relevant French companies need to establish in order to have "effective" compliance programs under the French anti-corruption law, the Loi Sapin II.

7.3.3 Although these guidance publications were developed in order to inform the evaluation of corporate risk-mitigation measures in criminal law (anti-corruption) contexts, they provide helpful indications as to the elements expected by leading enforcement authorities of an effective corporate compliance programme generally. Apple has drawn inspiration from these leading global standards in considering the reasonableness, proportionality and effectiveness of risk mitigation measures needed in respect of the App Store.

7.3.4 The UK MoJ Guidance and the UK HMRC Guidance adopt a practical approach, focussing on six general guiding principles which should inform such compliance programmes: risk assessment, proportionality of risk-based mitigation measures; top level commitment within the company; due diligence; communication, including training; and monitoring and review. Apple has considered each of these elements in considering what is required to satisfy itself as to the reasonableness, proportionality and effectiveness of risk-mitigation measures in place in respect of the App Store.

7.3.5 The US DOJ Guidance takes a step back, and invites those assessing a corporate compliance programme to consider three questions:

(a) "Is the corporation's compliance program well designed?" Apple has considered this question when assessing the reasonableness and proportionality of the App Store risk mitigation measures detailed in Section 6.

(b) "Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively?" Apple has considered this question when assessing the proportionality and effectiveness of the App Store risk mitigation measures detailed in Section 6.

(c) "Does the corporation's compliance program work in practice?" Apple considered this question when assessing the effectiveness of the App Store risk mitigation measures detailed in Section 6. The DOJ Guidance notes that the question of effectiveness is a complex one, but recognises that no compliance program can be designed to address all breaches.

7.3.6 The French Anti-Corruption Agency's Guidelines take a more prescriptive approach, specifying necessary elements of an appropriate corporate anti-corruption compliance program, to include:

(a) a code of conduct;

(b) an internal whistleblowing mechanism;

(c) a corruption risk-mapping system;

(d) a third-party risk assessment process;

(e) internal and/or external accounting controls;

(f) training programs for employees exposed to higher risk;

(g) a disciplinary procedure for breaches by employees; and

(h) an audit mechanism.

7.3.7 As regards DSA compliance-related risk mitigation measures in respect of the App Store, elements (c), (d) and (h) from this list are an integral part of the mandatory requirements for VLOPs under Articles 34 and 37; (b) is reflected in the various notice and actions mechanisms relevant to the App Store, including, inter alia, Report a Problem and Report a Concern; (f) is reflected in both the existing training provided to App Reviewers and content moderation specialists (to be supplemented with DSA-specific training provided to such personnel on the Systemic Risks); and (a), (e) and (g), while not relevant to Systemic Risk mitigation, find analogues in, respectively, the Guidelines, Apple's ongoing App Review of live apps and content moderation; and Apple's active enforcement of the Guidelines in the event of violation.

### 7.4 Reasonableness, proportionality and effectiveness of the risk mitigation measures designed to address the Systemic Risks identified in Section 5

7.4.1 Below, Apple addresses the reasonableness, proportionality and effectiveness of its risk mitigation measures that apply to the Systemic Risks identified in Section 5.

7.4.2 Apple notes at the outset that the scale and comprehensiveness of the risk mitigation measures applicable to the App Store strongly support the view that the risk mitigation measures are reasonable and proportionate. It is Apple's commercial imperative to keep the App Store a safe and trusted place and it invests heavily in its risk mitigation measures to achieve this.

7.4.3 The DSA provides no meaningful indication as to the standard against which the effectiveness of risk mitigation measures is to be assessed, nor is there a ready analogue in other EU compliance obligations. Against this background, some inspiration may be drawn from the *acquis communautaire,* informed by the case law of the European Court of Human Rights, in relation to the right to an effective remedy for government violation of such rights under Article 47 of the Charter and Article 13 of the European Convention on Human Rights and Fundamental Freedoms. The settled jurisprudence on the right to an effective remedy focuses on there being a remedy capable of leading to the identification and resolution of a violation, and acknowledges that there is no requirement that the remedy go so far as to being capable of preventing the breach arising. In sum, the jurisprudence requires national courts to strike an appropriate, proportionality-based balance between the need to secure EU law rights in the national legal order and the application of domestic procedural and remedial rules. In Apple's view, the risk mitigation measures it deploys are effective, and strike the appropriate balance between the interests at stake in connection with the Systemic Risks and any other countervailing considerations, and effectively address the risks identified.

7.4.4 It bears repeating here that the following controls operate to address each of the Systemic Risks identified in Section 5, or to the extent any of those risks conflict, to effectively strike a balance.

7.4.5 First, both developers and users who engage with the App Store are subject to clear written terms, which are available online. Users' engagement with the App Store is governed by the AMS Terms, which provide a basis for Apple to take action against a user who does not comply. Developers' engagement with the App Store is governed by the ADA and DPLA, which are similarly readily enforceable against non-compliant developers. Both of these agreements clearly set out Apple's expectations with respect to security, privacy, performance, user safety and product integrity. Again, these documents provide Apple with a clear basis for taking action against developers who do not comply.

7.4.6 Second, all developers who want to publish apps on the App Store are subject to developer screening measures, both at onboarding and on an ongoing basis. The enrolment screening process helps Apple stop fraudulent or sanctioned developers from developing and distributing apps that may contain illegal or harmful content from gaining access to the App Store. Some malicious developers try to regain access to the App Store and developer screening measures serve as an important gateway to keep them off or remove them from the App Store.

7.4.7 Third, the Guidelines set a clear and transparent standard for all apps and app updates that will be published on the App Store. The Guidelines are subject to periodic review, updates, and additions, which offer opportunities to enhance the Guidelines and address risk generally, including the Systemic Risks.

7.4.8 Fourth, all apps and app updates published on the App Store are subject to two levels of review. First, automated review gathers information that can be interpreted by machine learning algorithms and analysed for threats and signals (for example, the presence of malicious URLs or executable code) that provide relevant app information to the human review component. Second, all apps are subject to human review, where app reviewers analyse the signals provided by automated systems and review the features and functionality of apps to ensure they are compatible with the App Store's systems and products, comply with the Guidelines, and do not give signs of potential deceptive, abusive, or otherwise harmful behaviour.

7.4.9 A team of over 500 human app reviewers rigorously enforce the Guidelines. Their work is subject to ongoing monitoring and review. On a daily basis, the App Review team escalates app issues to senior management in the App Review team and the App Store Legal team. Certain issues are escalated to the ERB for consideration.

7.4.10 Fifth, even after apps are approved for publication on the App Store, they are subject to ongoing monitoring. Apple has a number of automated tools in place to detect malware on existing apps, that it runs at periodic intervals to capture content at different times. This includes tools to identify "bait-and-switch" apps, where apps available on the App Store change or add new functionality after approval by the App Review team.

7.4.11 Sixth, for published apps, the App Store provides avenues for consumers, developers, government authorities and others to provide notices and alerts of potential problems or concerns with apps or app content, and numerous teams within the App Store can and do act on these concerns. This includes the new DSA Content Reports portal.

7.4.12 As noted at paragraph 5.11.2 above, there is inevitably some measure of risk arising from the fact that the existing risk mitigation measures in place cannot be expected to have a 100% success rate to mitigate the Systemic Risks which may stem from the App Store, particularly as the nature of threats evolve. However, given that controls exist at different stages of the app lifecycle, these proactive and reactive steps ensure that threats to users who engage with the App Store are actively minimised.

## *(a) Article 34(1)(a) – Dissemination of Illegal Content*

### (i) Risk profile

7.4.13 As noted in Section 5, there is a material risk that, absent appropriate risk mitigation measures, the App Store could be used to disseminate illegal content to users in the EU. This includes the App Store being used to facilitate the infringement of intellectual property rights, and apps that facilitate fraud and other illegal behaviours, or defamatory material.

7.4.14 With respect to users, Apple has concluded that the risk that App Store-hosted UGC may give rise to the dissemination of illegal content is low to moderate.

### (ii) Terms and Conditions and Applicable App Review Guidelines

7.4.15 The Submission Guidelines in the AMS Terms clearly prohibit the posting of objectionable, offensive, unlawful, deceptive, inaccurate or harmful content by users in ratings and reviews.

7.4.16 The DPLA also clearly prohibits developers from using the App Store to disseminate illegal content. The DPLA expressly provides that developers must not use the App Store to engage in unlawful or illegal activity, develop products which would commit an offence or facilitate the commission of a crime or civil wrong, threaten, incite or promote violence or terrorism, or other serious harm, create or distribute any content or activity that promotes CSAM, or that violates, misappropriates or infringes on the intellectual property rights of others.

7.4.17 Section 1.1 of the Guidelines prohibits objectionable content, including defamatory content.

7.4.18 Section 4.1 of the Guidelines prohibits apps which impersonate other apps or services.

7.4.19 Section 5 of the Guidelines states apps must comply with all legal requirements in any location where developers make them available, and specifies that the developer is responsible for understanding and ensuring their app conforms with all local laws.

7.4.20 In addition, Section 5 notes apps that solicit, promote or encourage criminal or clearly reckless behaviour are unacceptable, and warns that in extreme cases, such as apps that are found to facilitate human trafficking and/or the exploitation of children, the appropriate law enforcement authorities will be notified.

7.4.21 Section 5.2 requires developers to only include content in their app if they own it or are licensed or otherwise have permission to use it.

7.4.22 The Apple Search Ads terms and conditions also require developers to ensure that Apple Search Ads are legal in the country in which the ads will be presented to users.

### (iii) App Review

7.4.23 Both automated review and human app review consider app submissions for illegal content. With respect to automated review, this includes for example URL detection which analyses URLs that have been previously flagged for illegal or harmful content or characteristics. Post-publication, these automated systems also detect bait-and-switch tactics, which can facilitate illegal conduct. Human app reviewers also review each and every app submission and app update for potential legal issues and risks, including unlicensed content, CSAM, real money gaming, and terrorist content.

### (iv) Additional specific controls

7.4.24 App Store fraud mitigation measures address the risk of the App Store being used to facilitate fraud. These measures include different forms of fraud detection and in 2022 prevented over USD two billion in fraudulent transactions.

7.4.25 The AMS Content Disputes process provides a mechanism for third parties to submit content disputes relating to the App Store via a dedicated webpage. Although the parties to the dispute are primarily responsible for its resolution, the AMS Contents Disputes team can and does intervene, particularly in cases where the developer has been the subject of multiple complaints or where there is a reasonable indication that an IP violation has occurred.

7.4.26 For apps live on the store, the App Store provides avenues for consumers, developers, government authorities and others to provide notice of potential problems or concerns with apps or app content that may be illegal. This includes the new Content Reports portal. Escalation mechanisms exist to ensure that apps comply with the Guidelines and local law, and are removed where there are violations.

7.4.27 Notwithstanding that the risk that App Store-hosted UGC may give rise to the dissemination of illegal content is low to moderate, all ratings and reviews are subject to content moderation. This includes proactive measures including automated scanning of all ratings and reviews, and reactive measures in circumstances where Apple is made aware of problematic ratings and reviews. In situations where ratings and reviews are escalated for further investigation, for example in cases where a reported concern relates to a rating and review that contains malicious activity that infers bodily harm, or child safety and / or child exploitation concerns, these are addressed, for example by Global Security Investigations, and may result in a report to law enforcement.

### (v) Effectiveness

7.4.28 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.

7.4.29 Examples of apps recently removed or rejected from the App Store due to illegal content include an app with defamatory and antisemitic language in the metadata and an app listed all Wi-Fi hotspots in the app with offensive and homophobic titles (rejected under Guideline 1.1 for Objectionable content), an app impersonating the app of a verified developer (rejected under Guideline 4.1 for Copycat violations) and an app that used unlicensed song lyrics and also appeared to use a copycat user interface (rejected under Guideline 5.2 on Piracy).

7.4.30 Given the limited risk profile of Apple Search Ads, Apple considers its relevant terms and conditions and their enforcement are adequate to address any Systemic Risks engaged by Apple Search Ads.

### *(b) Article 34(1)(b) – Actual or foreseeable negative effects on rights to human dignity and respect for private and family life, enshrined in Articles 1 and 7 of the Charter*

#### (i) Risk profile

7.4.31 As noted in Section 5, absent appropriate risk mitigation measures, the likelihood of developers seeking to publish apps capable of engaging the rights to human dignity and respect for private and family life in such a way as to give rise to Systemic Risks would be high, and the severity of such risks could vary from modest to extreme (for example, in the cases of CSAM, so-called "revenge pornography", or "deepfakes").

#### (ii) Terms and Conditions and Applicable App Review Guidelines

7.4.32 The Submission Guidelines in the AMS Terms and Conditions clearly prohibit the posting of objectionable, offensive, unlawful, deceptive, inaccurate or harmful content by users in ratings and reviews.

7.4.33 The DPLA also clearly prohibits developers from using the App Store to engage in unlawful or illegal activity; threaten or incite violence, terrorism, or other serious harm; or create or distribute any content or activity that promotes child sexual exploitation or abuse.

7.4.34 Section 1.1.1 of the Guidelines (Safety) prohibits apps that contain defamatory, discriminatory, or mean-spirited content, 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.

7.4.35 Section 1.1.2 prohibits realistic portrayals of people being killed, tortured or abused, or content that encourages violence.

7.4.36 Section 1.1.3 prohibits depictions that encourage violence, or illegal or reckless use of weapons.

7.4.37 Section 1.1.4 prohibits overtly sexual or pornographic material. This includes "hookup" apps and other apps that may include pornography or be used to facilitate prostitution, or human trafficking and exploitation.

7.4.38 Section 1.1.7 prohibits apps that contain harmful concepts which capitalise on current events.

7.4.39 Section 1.2 of the Guidelines requires apps with UGC to include methods for filtering objectionable content, mechanisms for reporting offensive content, the ability to block offensive users from the service, and published developer contact details. It also provides that apps with UGC or services that end up being used primarily for pornographic content, Chatroulette-style experiences, objectification of real people (for example "hot-or-not" voting), making physical threats, or bullying may be removed from the App Store without notice.

7.4.40 Section 1.4 of the Guidelines warns that apps that present risks of serious harm may be rejected.

7.4.41 Section 5 of the Guidelines (Legal) notes apps that solicit, promote, or encourage criminal or clearly reckless behaviour are unacceptable, and warns that in extreme cases, such as apps that are found to facilitate human trafficking and / or the exploitation of children, the appropriate authorities will be notified.

### (iii) App Review

7.4.42 Both automated review and human app review consider app submissions that may engage these rights, although given their nature, apps submissions that have actual or foreseeable negative effects on these rights are more likely to be addressed via human review.

### (iv) Additional specific controls

7.4.43 Where the App Store is alerted to risks of CSAM being disseminated on apps that are available on the App Store, they escalate issues to Child Safety Counsel (see paragraphs 6.8.7 to 6.8.8 above). All such escalations are investigated and if appropriate notified to law enforcement.

7.4.44 To the extent that suspected criminal offences involve threats to the life or safety of a person or persons as envisaged by Article 18 of the DSA engage the right to right to human dignity, the new Article 18 procedures applicable to the App Store are designed to ensure that law enforcement authorities in the Member States concerned are notified in a timely manner.

7.4.45 Where new or novel issues involving human dignity are identified, they are escalated to App Review Policy and other teams for consideration.

### (v) Effectiveness

7.4.46 The App Store considers and takes action against apps that give rise to actual or foreseeable negative effects on rights to human dignity and respect for private and family life. For example, Guideline 5 Legal: has recently been used to consider apps giving rise to risk of use for the purposes of modern slavery, including child labour, and human trafficking; to remove video call and chatroom apps identified as carrying CSAM content; and to address apps incorporating social media features which are identified as being used for bullying, threats and other abuse.

### *(c) Actual or foreseeable negative effects on developers' and users' rights to the protection of personal data enshrined in Article 8 of the Charter*

#### (i) Risk profile

7.4.47 As noted in Section 5, absent risk mitigation measures, there would be a significant risk that there could be negative effects on developers' and users' rights to the protection of their personal data.

#### (ii) Terms and Conditions and Applicable App Review Guidelines

7.4.48 Section 5 of the Guidelines (Legal) makes clear that protecting user privacy is paramount in the Apple ecosystem. It also prohibits developers from using, transmitting or sharing a user's personal data without first obtaining their permission, and requires developers to provide access to information about where and how a user's personal data will be used. Explicit permission must be obtained from the user in order to track their activity, via the App Tracking Transparency API.

7.4.49 The DPLA also requires developers and their apps to 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).

7.4.50 The Submissions Guidelines in the AMS Terms also clearly prohibit the posting of personal, private or confidential information belonging to others, or requesting personal information from a minor.

7.4.51 Section 5 of the Guidelines (Legal) warns that apps which share user data without user consent or which otherwise do not comply with data privacy laws may be removed from sale, and may also result in the developer's removal from the Apple Developer Program.

7.4.52 In addition, the App Store & Privacy Notice ensures that users have an effective choice and any consent to data use on Apple products is fully informed. Apple's Data & Privacy Icon also provides users with transparent and easily accessible information that details how Apple collects, processes and discloses their personal data.

#### (iii) App Review

7.4.53 Both automated review and human review consider app submissions for privacy protections and compliance with Apple's privacy requirements. For example, automated review involves checks [CONFIDENTIAL]. Human reviewers then consider [CONFIDENTIAL], including permission requests to seek the user's permission for such access, are consistent with the purported functionality and purpose of the app. They also ensure that developers have complied with all privacy- related Guidelines requirements, including requirements to publish privacy policies.

#### (iv) Additional specific controls

7.4.54 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 users' data, such as a user's location, browsing history, and contacts.

7.4.55 App Privacy Reports enable users to see how often their location, photos, camera, microphone, and contacts have been accessed by apps during the last seven days, and which domains those apps have contacted. Users therefore have full and easy visibility into the ways apps use the privacy permissions a user has granted them, as well as their respective network activity.

7.4.56 Developers who want to track a user across apps and websites or access their device's data for advertising purposes must seek the user's permission through the App Tracking Transparency Framework. This applies across all apps available on the App Store, including Apple's own apps.

7.4.57 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.

7.4.58 Users are able to determine whether they receive personalised recommendations when they are discovering apps on the App Store. 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.

#### (v) Effectiveness

7.4.59 With specific respect to the right to protection of personal data, in addition to the measures above, the effectiveness of Apple's risk mitigation measures is ensured firstly by Apple's ongoing compliance with GDPR, and secondly by putting users firmly in control of the management of their own data when using the App Store. In accordance with Article 24 of the GDPR, the measures implemented by Apple take account of the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. These measures are subject to continuous review.

### *(d) Actual or foreseeable negative effects on the rights of developers and users to freedom of expression and freedom of information, including the freedom and pluralism of the media, under Article 11 of the Charter*

#### (i) Risk profile

7.4.60 As noted in at Section 5 above, while such risks to freedom of expression and information may conceivably arise in connection with the App Store, the probability of negative effects on these rights arising in practice can only reasonably be seen as remote; and their impact, should they arise, modest.

7.4.61 As regards the freedom and pluralism of the media, as noted at paragraph 5.7.13, notwithstanding the risk of abusive governmental takedown demands, the risk of negative impacts on pluralism of the media in the EU stemming from the App Store is, on any objective analysis, low.

### (ii) Terms and Conditions and Applicable App Review Guidelines

7.4.62 The Introduction to the Guidelines states clearly that Apple strongly supports all points of view being represented on the App Store, as long as the apps are respectful to users with differing opinions and the quality of the app experience is high.

7.4.63 Apple notes that such is its commitment to pluralism of the media that it uniquely and exceptionally exempts professional political satirists and humourists from its prohibition in Guideline 1.1.1 on defamatory, discriminatory, or mean-spirited content, including references or commentary about religion, race, sexual orientation, gender, national / ethnic origin, or other targeted groups.

7.4.64 The AMS Terms permit users to post reviews of apps they have downloaded, provided they comply with the Submissions Guidelines, such restrictions being designed to keep the App Store a safe and trusted place for all.

### (iii) App Review

7.4.65 All apps will be admitted to the App Store unless they are illegal or in violation of the DPLA or Guidelines, which are publicly available. Where app submissions raise novel human rights issues, including issues that engage freedom of expression, they can be escalated as appropriate to the various support teams that support App Review, including App Review Policy, the App Store Legal team, and if necessary the ERB. When apps are rejected, developers have a resource to challenge rejection decisions via the appeals process.

### (iv) Additional specific controls

7.4.66 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 Section 6 above. The App Store Legal team and other functions assess whether the app complies with the Guidelines, and whether the request is in accordance with local law (both as to substance as well as whether the agency has the authority to make the request). App Store Legal will in some instances consult with local counsel on the legality of the request. The App Store Legal team can also escalate requests to the ERB for consideration. If a request is in accordance with local law the media app may be removed form a local App Store Storefront. Requests that are not in accordance with local law would only be actioned if the app otherwise violated the Guidelines.

#### (v) Effectiveness

7.4.67 A broad range of views and opinions from across the EU are available on the App Store. The App Store risk mitigation measures balance the tension between freedom of expression and the need to keep users safe.

7.4.68 A very broad range of media voices across the EU are present on the App Store. Consideration of the issue of media pluralism by the UK's specialist communications and media regulator, Ofcom, has not identified concerns for media pluralism stemming from the App Store. Apple is not aware of material concerns being raised in any other quarter with respect to negative effects in the EU for media pluralism stemming from the App Store. In those circumstances, Apple has no reason to believe that its risk mitigation measures are anything other than effective with respect to mitigating the risk of actual or foreseeable negative effects for the exercise of freedom of expression and information, and for media pluralism.

### *(e) The right to non-discrimination under Article 21 of the Charter*

#### (i) Risk profile

7.4.69 As noted in Section 5 above, Apple does not discriminate against developers or users, including when conducting developer screening, App review, or responding to notices and actions (including from law enforcement). As regards app recommendations and Apple Search Ads, if a user has personalisation turned on, age, gender and location are used to present personalised content, but such conduct does not amount to discrimination.

7.4.70 As regards developer use, although discriminatory content is clearly prohibited under the Guidelines, there is a risk that users could be exposed to such content in the App Store if it were not identified during the App Review process. However, app reviewers are trained to identify such content, and the notices and actions and complaints mechanisms provide means to raise relevant concerns regarding apps that are already published on the App Store.

#### (ii) Terms and Conditions and Applicable App Review Guidelines

7.4.71 Section 1.1.1 of the Guidelines (Safety) prohibits apps that contain defamatory, discriminatory, or mean-spirited content, 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.

7.4.72 The Developer Code of Conduct 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.

#### (iii) App Review

7.4.73 As part of the App Review process, human app reviewers ensure that app metadata, including text and images that will appear on the App Store comply with the Guidelines, including those relevant provisions listed above.

#### (iv) Effectiveness

7.4.74 Apple is not aware of any concerns from developers or users that Apple discriminates against them when attempting to gain access to the App Developer Program.

7.4.75 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. Examples of apps rejected or removed for violating the Guideline prohibition on discriminatory content include an app that had defamatory and antisemitic content in the app metadata, an app that included racist, homophobic and other derogatory posts, and an app that referred to certain groups as Nazis.

### *(f) Actual or foreseeable negative effects on the rights of the child enshrined in Article 24 of the Charter (addressing also the risk of negative effects in relation to the protection of minors, under Article 43(1)(d))*

#### (i) Risk profile

7.4.76 As noted in Section 5, absent appropriate risk mitigation measures, the App Store could give rise to, or be used in a manner giving rise to, risks of actual or foreseeable negative effects for the exercise of the rights of the child under Article 24 of the Charter.

#### (ii) Terms and Conditions and Applicable App Review Guidelines

7.4.77 The AMS Terms set out the requirements for "Family Sharing" accounts. The "family organizer" must be 18 or an equivalent age of majority in their country or territory of residence, and the parent or legal guardian of any users under age 13 (or equivalent age in their country or territory of residence). The terms also explain how purchase sharing works, and the ways in which eligible content is shared among members of a family, including the "Ask to Buy" feature.

7.4.78 The Submissions Guidelines in the AMS Terms prohibit various forms of misuse, including using the App Store to request personal information from a minor.

7.4.79 Section 2.4 of the Schedules to the DPLA 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.

7.4.80 The introductory section to the App Review 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."*

7.4.81 Section 1.3 (Kids category) provides that apps in the "Kids" category must not include links out of the app, purchasing opportunities, or other distractions to kids unless reserved for a designated area behind a "parental gate".[68] In addition to complying with privacy laws applicable to children, Kids Category apps may not send personally identifiable information or device information to third parties and should not include third-party analytics or third-party advertising.

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

7.4.83 Section 5.1.4 addresses personal privacy and data requirements for children: apps must comply with all children data protection laws (for example GDPR); apps should not include third-party analytics / advertising if intended for kids; use of terms like "For Kids" and "For Children" is reserved for the Kids Category; and apps not in the Kids Category cannot imply the app is for children.

### (iii) App Review

7.4.84 As part of the App Review process, human app reviewers assess whether apps align with the age ratings guidelines, and if a developer has submitted a proposed app to feature in the Kids Category, to assess that the app meets the Kids Category guidelines.

### (iv) Additional specific controls

7.4.85 All privacy-related controls listed above apply to minors.

7.4.86 Where the App Store is alerted to risks of CSAM being disseminated on apps that are available on the App Store, they escalate issues [CONFIDENTIAL] (see paragraphs 6.8.7 to 6.8.8 above). All such escalations are investigated and if appropriate notified to law enforcement.

7.4.87 Apple Search Ads is built with strong limitations to protect children and minors. For example, for a minor under 18 (or the age of majority in the relevant jurisdiction) who is logged in with their Apple ID account, the Personalised Ads setting is automatically set to "off" and cannot be enabled until the user reaches the age of majority. Furthermore, age ratings and the age of the user determine whether or which Apple Search Ads will be displayed to users under 18 years of age; Apple Search Ads are not presented to users under the age of 13; apps rated 17+ are not presented to users under 18 as Apple Search Ads.

### (v) Effectiveness

7.4.88 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

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

maintains controls to ensure that they are protected. Apple has created device level controls, such as Screen Time, to give parents control over apps that their children can download and use on their devices.

7.4.89 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 is subject to the 4+ age rating requirement.

7.4.90 A very significant number of apps are rejected after App Review due to concerns relating to minors. This includes for example dating apps targeted at minors, apps intended for children with educational and quiz type features that allow users to communicate without a "parental gate" control, apps that fail to comply with applicable privacy laws for minors, apps with public chat room access, and apps intended to connect users which require them to state their age, body type and gender preferences.

7.4.91 Apple's verification system for Apple IDs created for children is appropriate, when viewed in conjunction with 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). This is particularly so given that the App Store is not a social media service, a service that seeks or offers validation, or which uses children's data to create extensive profiles for advertising purposes. Apple does not collect unnecessary data that would determine how old a user is, but offers numerous other protections that apply to children.

7.4.92 Apple will continue to monitor the EU BIK+ strategy, including the ongoing work relating to an EU code of conduct on age-appropriate design.

### *(g) High level of consumer protection, enshrined in Article 38 of the Charter*

7.4.93 As noted Section 5 above, 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 Section 6 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.

### *(h) Actual or foreseeable negative effects on electoral processes*

#### (i) Risk profile

7.4.94 While online platforms can be used to disseminate false information which may give rise to risk relating to electoral processes, the likelihood of the App Store being used for such purposes is very substantially lower than for online platforms focussing primarily on UGC. Indeed, Apple considers the risk in this respect to be low in absolute terms.

### (ii) Terms and Conditions and Applicable App Review Guidelines

7.4.95 The AMS Terms prohibit manipulating play counts, downloads, ratings, or reviews via any means — such as (i) using a bot, script, or automated process; or (ii) providing or accepting any kind of compensation or incentive.

7.4.96 The Introduction to the Guidelines states clearly that Apple strongly supports all points of view being represented on the App Store, as long as the apps are respectful to users with differing opinions and the quality of the app experience is high. Any app including content or behaviour which violates Apple's policies or terms will be rejected.

7.4.97 Additional Guidelines requirements detailed above that relate to illegal content and human dignity are also relevant here.

### (iii) App Review

7.4.98 The App Review teams are vigilant to the issues presented around electoral processes, and work to exclude apps which are expected to be used to propagate harmful, misleading or deceptive information in connection with such processes, or apps that present themselves as official campaign apps, poll worker apps, or election resource app.

### (iv) Additional specific controls

7.4.99 During an electoral cycle in any given country, the App Review team maintains particular vigilance with a view to ensuring that apps engaging concerns are appropriately escalated. Relevant determinations are passed downstream to recommender systems and editorial teams to ensure that only relevant and legitimate apps relating to electoral processes are being surfaced for users in stories, or in recommendations.

7.4.100 Where events in a particular country or in connection with a particular event or situation give rise to specific concerns regarding potential disinformation or attempts to interfere with electoral processes, various App Store support functions, such as App Review Policy, the App Store Legal team, or the ERB, coordinate in order to ensure that new and emerging issues can be addressed. This may result in updated guidance to App Store support teams, including the App Review team and local editorial teams.

7.4.101 The country teams responsible for any particular App Store storefront are highly attuned to political trends and events in their countries of responsibility, and factor considerations relevant to electoral processes into editorial decisions.

### (v) Effectiveness

7.4.102 Apple considers that, 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 electoral processes.

### *(i) Actual or foreseeable negative effects on civic discourse and public security (including disinformation)*

#### (i) Risk profile

7.4.103 The App Store does not give rise to the risk of negative effects on civic discourse and public security to the extent remotely comparable with those online platforms whose design, function and / or use involve the widespread dissemination and rapid amplification of content, including UGC or news.

7.4.104 The risk that user ratings or reviews of apps hosted on the App Store may negatively affect civic discourse, electoral processes, or public security, is low.

7.4.105 Apple notes in this respect the balance to be struck between protection of civic discourse against disinformation (particularly where such disinformation may give rise to material harmful effects to the public) and the protection of freedom of expression and information, including media pluralism.

#### (ii) Terms and Conditions and Applicable App Review Guidelines

7.4.106 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.

7.4.107 Those Guidelines provisions listed above in respect of the rights to human dignity and respect for private and family life, and freedom of expression, are also relevant to negative effects on civic discourse and public security.

#### (iii) App Review

7.4.108 The App Review process, including its ongoing review of live apps, includes controls designed to identify apps intended to have an adverse impact on civic discourse, for example those apps designed to disseminate extremist content or disinformation. In practice, Apple enforces its applicable terms and conditions in relation to matters capable of adversely affecting civic discourse, such as inclusion of illegal content, pandemic disinformation, or terrorist content.

#### (iv) Additional specific controls

7.4.109 The additional specific controls listed above at paragraph 7.4.93 et seq. in respect of negative effects on electoral processes apply also in the case of negative effects on civic discourse and public security.

#### (v) Effectiveness

7.4.110 Apple considers that the provisions referred to above 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.

### *(j) Actual or foreseeable negative effects on gender-based violence*

#### (i) Risk profile

7.4.111 As stated in Section 5 above, the risk of the App Store being used to disseminate apps having a potential adverse effect on gender-based violence, the probability of such risks crystallising and the potential impacts that may flow therefrom, are similar to the risks described above with respect to illegal content.

#### (ii) Terms and Conditions and Applicable App Review Guidelines

7.4.112 The terms and conditions and applicable Guideline provisions listed above in respect of illegal content and the right to human dignity address negative effects on gender-based violence. Notably:

(a) Section 1.1.1 of the Guidelines clearly prohibits content on the App Store that is defamatory, discriminatory or mean-spirited, including references or commentary about religion, race, sexual orientation, gender, national / ethnic origin, or other targeted groups. This is particularly the case if the app is likely to humiliate, intimidate or harm a targeted individual or group.

(b) Section 1.1.2 of the Guidelines prohibits realistic portrayals of people or animals being killed, maimed, tortured or abused, or content that encourages violence. The App Store's relevant controls include these and other clear Guideline prohibitions, and the removal of apps identified as giving rise to such risk and the ability to alert law enforcement authorities.

#### (iii) App Review

7.4.113 Apple refers to the App Review practices identified above with respect to: (1) the dissemination of illegal content; and (2) the rights to human dignity, and to private and family life.

#### (iv) Additional specific controls

7.4.114 Apple refers to the specific controls identified above with respect to: (1) the dissemination of illegal content; and (2) the rights to human dignity, and to private and family life.

#### (v) Effectiveness

7.4.115 Apple considers that its assessments at paragraphs 7.4.27 *et seq.* and 7.4.43 *et seq.* above as to 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.

### *(k) Actual or foreseeable negative effects on public health, serious negative consequences to a person's physical and mental well-being*

#### (i) Risk profile

7.4.116 As noted at section 5.9(e) above, risks to public and individual health do not arise from the use of the App Store in a manner or to an extent comparable with other online platforms with business models focussing on widespread dissemination and rapid amplification of UGC. In general, Apple considers the risk profile of the App Store in this respect to be, objectively, no more than modest, while nonetheless acknowledging that were such risks to crystallise, their impact could be significant.

7.4.117 In light of the UGC content moderation controls, the risk that user ratings or reviews of apps hosted on the App Store may produce negative effects on public health and physical and mental well-being is low. Apple has 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, those controls are set to "on" by default or are readily available to parents to facilitate the safety of children.

7.4.118 As regards UGC, clearly, the risk of user ratings or reviews of apps hosted on the App Store may produce negative effects on public health and physical and mental well-being is low.

#### (ii) Terms and Conditions and Applicable App Review Guidelines

7.4.119 The AMS Terms prohibit users from posting objectionable, offensive, unlawful, deceptive, inaccurate, or harmful content in ratings and reviews.

7.4.120 The Guidelines contain multiple rules that address physical health and well-being. For example:

(a) Section 1.4 of the Guidelines addresses app behaviour that risks physical harm.

(b) Section 1.4.1 specifically addresses "medical apps".

(c) Section 1.4.2 specifically addresses "drug dosage calculators".

(d) Section 1.4.3 specifically addresses apps that "encourage consumption of tobacco and vape products, illegal drugs or excessive amounts of alcohol".

(e) Section 1.4.5 provides that apps should not urge customers to participate in activities (like bets, challenges, etc.) or use their devices in a way that risks physical harm to themselves or others.

#### (iii) App Review

7.4.121 App Review seeks to ensure that all app submissions comply with the Guidelines above.

### (iv) Additional specific controls

7.4.122 Engagement with the App Store does not give rise to addiction issues that have the potential to cause serious negative consequences to a person's physical and mental well-being. To the extent that such risks arise outside of the App Store after users download apps, Apple's Screen Time functionality, referred to in Section 3, can be used by adults and vulnerable and minor users to track and control the time they are spending on particular apps.

7.4.123 Apple notes in passing that its requirement in the Guidelines (Guideline 1.2) for apps with user-generated content or social networking services to include arrangements for filtering objectionable material, reporting offensive content, and blocking abusive users provide helpful mitigation in respect of risks in this category arising from third-party apps.

7.4.124 All ratings and reviews are subject to controls to ensure that they comply with the Submissions Guidelines, including to ensure that they do not contain objectionable, offensive, unlawful, deceptive, inaccurate, or harmful content.

### (v) Effectiveness

7.4.125 Apple considers its risk mitigation measures to provide it with sufficient means to take action against threats to public or individual health which may arise in connection with the App Store.

## SCHEDULE A: RELEVANT TEAMS AND FUNCTIONS REFERENCED IN THE REPORT[69]

| Team / Function and overview of role |
|---|
| **AMS Content Disputes Legal**<br>The AMS Content Disputes Legal team was put in place to address and help mitigate intellectual property, and other third-party rights violations on the App Store, prevent the removal of content due to fraudulent or anticompetitive claims, and limit liability to the App Store. The AMS Content Disputes Legal team puts claimants in direct contact with the provider of the disputed app. If needed, claimants 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. |
| **App Review**<br>The App Review function consists of multiple teams who contribute to keeping the App Store a safe and trusted place to discover apps.<br>The function consists of teams involved in automated and human app review, as well as review escalations.<br>***Automated review – Engineering***<br>Engineering teams, including Apple's infrastructure and machine learning teams, are responsible for developing different tools used in static binary analysis, asset analysis, and runtime analysis [CONFIDENTIAL].<br>***App Review Support Specialists and App Review Escalations***<br>Apple's App Review team consists of over 500 human experts, including App Review Support Specialists and App Review Escalations. The App Review organisation includes a team of App Review specialists who review third-party developer apps, as well as a Content and Communications function in that works on ensuring that any new policies or workflows are documented and shared with reviewers.<br>App Review Escalations is staffed by teams of senior reviewers in specialised areas, including Policy Escalations, App Review Compliance, Developer Advocacy and Technical Investigations. Additionally, the App Review Business Excellence team's focus is performing quality control and auditing functions to conduct root-cause analysis and make necessary improvements, whether to tools or performance management of reviewers. |

[69] This is not and is not intended to be an exhaustive list of every team at Apple that carries out work in connection with the operation of the App Store, or its related risk mitigation measures.

| Team / Function and overview of role |
|---|
| **App Review Board**<br>The App Review Board is composed of experienced App Review specialists who investigate claims asserted in an appeal and the history of the app and interactions with the developer, and who seek input from specialised functions where appropriate. |
| **App Store Editorial team**<br>The App Store Editorial team is responsible for curating content, including recommending apps, on the App Store. This is a global team, with personnel based in the EU and elsewhere. |
| **App Store Legal**<br>The App Store Legal team is a team of in-house counsel with global coverage who have primary responsibility for all legal and regulatory issues relevant to the App Store. The team has day-to-day responsibility for reviewing, authoring and updating key App Store policies, including the App Review Guidelines and Apple Developer License Agreement. It works closely with a number of teams that have responsibility for aspects of the App Store, including App Review, Recommender Systems, Privacy Compliance, Privacy Legal and Global Security Investigations. It receives internal escalations from various App Review and other teams who need legal and regulatory advice, and is responsible for the dedicated notices and actions email addresses used by government agencies and law enforcement authorities. It is also responsible for AMS Content Disputes. |
| **Apple Search Ads**<br>The Apple Search Ads Policy team develops and enforces policies governing advertising placements, and ensures that they are driven by compliance with regulations. The team also ingests, reviews and resoles disputes raised via customer communications regarding Apple Search Ads.<br>The Ad platforms, Privacy and Compliance Engineering team works with policy and privacy teams to put advertising restrictions and privacy controls in place, and regularly conducts testing to validate the effectiveness of automated controls. |
| **AppleCare**<br>AppleCare provides global support for Apple services, including the App Store, and has specialised teams that support the App lifecycle at various points. AppleCare deals primarily with external escalations, [CONFIDENTIAL] such as Report a Problem.<br>AppleCare Support Engineering plays a role in monitoring customer feedback to improve the quality of products and services. The team functions as the conduit through which most interactions with the Apple Media Products ("AMP") organisation |

| Team / Function and overview of role |
|---|
| (which includes the App Store) takes place. The team is instrumental in bringing clear line-of-sight to AMP efforts and allows the entire AppleCare organisation to offer a consistent support experience. AppleCare Engineering team (ACE) focuses on three areas of Apple media products business: Product Readiness, Strategic Systems, and Product Support.<br>AppleCare Analytics and Reporting works on monitoring AppleCare's internal performance, and works closely with the AppleCare engineering team. The team monitors trends from customer calls across Apple service areas (i.e. # of customers calling because they have forgotten their password), if they notice spikes or trends in these areas, they escalate to the AppleCare Engineering team, who then reach out to the relevant areas (Engineering teams) to fix certain recurring issues that may stem from product / build errors.<br>AppleCare Contact Center: AppleCare has a variety of customer-facing support teams who provide both general and specialised support for various teams and products within the App Store. Examples include the Developer Program Support Team and AMP Moderation advisors. |
| **Child Safety Counsel**<br>Child Safety Counsel is a part of the Global Security and Investigations Team and is a dedicated resource tasked with investigating and responding to escalations regarding allegations of CSAM. |
| **EU Regulatory Legal**<br>The EU Regulatory Legal team provides advice to internal stakeholders on key EU legislation, primarily the Digital Markets Act and the Digital Services Act. It also manages legal engagement with the European Commission and other regulatory and Government agencies regarding EU legislation, including responding to regulatory enquires. |
| **Executive Review Board**<br>The Executive Review Board is composed of senior leaders who have ultimate decision-making responsibility regarding 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.<br>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. |
| **Global Security Investigations** |

| Team / Function and overview of role |
|---|
| Global Security Investigations is a resource for teams across Apple to escalate issues of child sexual abuse material, pro-terror, harassment or criminal content. Apple's Child Safety counsel functions as a liaison between Apple and local law enforcement, as they review escalated content across services and report qualifying criminal content to local law enforcement agencies, including the National Center for Missing and Exploited Children. Global Security Investigations partners with App Store Legal to manage legal requests from law enforcement agencies pertaining to the App Store, including app takedown requests. This team works closely with App Store Legal and App Review to review, investigate and respond to agency requests. |
| **Government Affairs**<br>Government Affairs is a global team that provides advice to internal stakeholders on relevant legislation and policy developments. In the EU, the EU Government Affairs team engages with internal stakeholders on EU legislation and policy, including the DSA. It also manages policy engagement with the European Commission as well as other regulatory, legislative and government agencies regarding EU and national legislation. |
| **Human Rights Legal**<br>The Human Rights Legal team implements Apple's Human Rights Policy across the organisation, including the App Store. Human Rights Legal works to put in place processes that can help identify potential human rights risk across business areas, and the means of addressing these risks. |
| **Privacy Compliance**<br>The Privacy Compliance team is primarily focused on Apple's obligations under applicable global privacy and data protection laws. It conducts privacy impact assessments and legitimate interest analyses, advises on data subject access requests and other requests from data subjects seeking to exercise their privacy rights, and strategies for complying with new privacy laws around the world. As part of privacy compliance, the privacy counselling team is primarily responsible for guiding the business as they navigate privacy issues around the world. The counselling team evaluates privacy risks in M&A, collaborates with counsel on the development of new and existing projects, and evaluates Apple's internal approach to privacy, among other efforts. The privacy counselling team partners closely with a number of teams, including Privacy Legal, Product Legal and Privacy Engineering. |
| **Privacy Legal**<br>The Privacy Legal team is responsible for day-to-day privacy product counselling and development. This includes understanding and advising on the privacy practices of the apps, features and functions that the privacy legal team supports, and assisting other privacy colleagues by serving as subject-matter experts for those apps, features and |

| Team / Function and overview of role |
|---|
| functions. The Privacy Legal team works closely with the business teams on building privacy compliant apps, features and functions that respect privacy by design principles and that meet or exceed privacy requirements under data protection laws around the world. The Privacy Legal team also partners closely with Product Legal, Privacy Compliance, Privacy Engineering, Privacy Product Marketing and the Law Enforcement teams in providing privacy counselling. |
| **Recommender Systems**<br>Recommender systems personalise content for customers based on their engagement and interaction with apps on the App Store. Prior to personalised recommendations on the App Store, the recommender systems distil a variety of automated and human signals received [CONFIDENTIAL], cross-reference the application [CONFIDENTIAL], and finally, upon verifying user consents and age restrictions, provide a personalised experience.<br>[CONFIDENTIAL]. |
| **Services Special Programs**<br>Services Special Programs manages programs and develops requirements for engineering and operations teams to effectively respond to global regulations of internet services. Its work includes efforts to implement changes mandated under the DSA. |
| **Trust & Safety**<br>***Trust & Safety Content & Discovery Fraud Team***<br>Apple Media Products Engineering aims to detect trust and safety concerns across App Store teams and customer feedback, and build automated pathways to address these concerns, while ensuring that they are escalated to the right teams. [CONFIDENTIAL].<br>***Trust & Safety Developer Fraud***<br>The Developer Fraud team works closely with World Wide Developer Relations and Trust and Safety Operations to detect and prevent illicit app distribution by fraudulent |

| Team / Function and overview of role |
|---|
| developers, and previously terminated developers from re-entering the App Store. The team conducts identity verification and other risk-based checking on developers at enrolment and works to detect any misuse of alternate app distribution channels or circumventions of the App Review process.<br>***Trust & Safety Evaluations***<br>The Trust and Safety Evaluations team conducts assessments and evaluates risk associated with all new features across the App Store. The team identifies potential vulnerabilities for the platform, and functionality that may be susceptible to fraud and abuse. The team proposes measures to address such issues and provides them in the form of recommendations to stakeholder teams.<br>***Trust & Safety External Partnerships***<br>The Trust and Safety External Partnerships team focuses on external engagement with various organisations regarding policy issues relevant to Apple's products and services, such as online safety and child safety. The team works with a variety of industry groups to solicit product feedback and identify trends and concerns.<br>***Trust & Safety Operations***<br>*Trust and Safety Operations aims to protect customer experience and ensure that the Apple ecosystem, including the App Store, is a trustworthy and safe environment. The team works to combat fraud accurately, promptly, and at scale across a variety of App Store functions, including developer enrolment, ratings and reviews, as well as app discovery.* |
| **World Wide Developer Relations**<br>Worldwide Developer Relations ("WWDR") manages the Apple Developer Program in partnership with Apple Trust & Safety Operations and Apple Developer Program Support (an offshoot of AppleCare). WWDR works to assist to assist developers with program enrolment, and also conducts developer risk assessment via identity screening, sanctions and fraud checks to prevent bad actors from entering the AppStore. |