23 September 2025

Feedback of

# ACT | The App Association
# (Transparency Reg. # 72029513877-54)
# Rue Belliard 40,
# 1000 Brussels, Belgium

to the

## European Commission

regarding the

## Review of the Digital Markets Act

## I. Introduction

ACT | The App Association (hereafter 'App Association') welcomes the opportunity to submit comments to the European Commission's consultation on the review of the Digital Markets Act.

The App Association is a policy trade association for the small business technology developer community. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. Today, the ecosystem the App Association represents—which we call the app economy—is valued at approximately €95.7 billion and is responsible for more than 1.4 million jobs in the European Union (EU).[1]

While the App Association's members are unlikely to ever be considered gatekeepers, their success is closely linked to a small and medium-sized enterprise (SME)-friendly implementation of the Digital Markets Act (DMA). The purpose of this document is to share the perspective of our member companies to help the Commission ensure, as it implements and enforces the DMA, that SMEs, startups, and scaleups can continue to thrive and innovate in the app ecosystem.

## II. Digital Markets Act

### a. List of Core Platform Services and designation of gatekeepers

The initial designation of gatekeepers under the DMA marks an important milestone in the implementation of the Regulation. However, we believe that the process to date has not sufficiently accounted for the diversity of business models among designated companies, nor for the practical implications for SMEs and users that rely on gatekeeper services. Recognising these differences is critical to ensuring that enforcement supports, rather than hinders, innovation and competition across the ecosystem.

The designation process did not adequately incorporate the perspectives of SMEs, even though they are among the most directly affected stakeholders. The obligations and prohibitions imposed on gatekeepers have consequences that extend beyond large platforms to the smaller businesses that depend on predictable and fair access to their services. Future designations should therefore be informed by a more inclusive process, with careful consideration of the impact on SMEs, users, and the wider business environment.

It is important that emerging technologies are not hastily included within the existing list of Core Platform Services (CPS). For example, AI is a foundational technology embedded across many digital services, not a standalone service. Expanding the CPS definition in this way would fall outside the original scope of the DMA and introduce regulatory uncertainty without clear benefits for SMEs or consumers.

[1] *See* 220912_ACT-App-EU-Report.pdf.

If AI were designated as a CPS, even small app developers that integrate third-party AI tools into their products would be affected by the compliance burdens designed for large gatekeepers. An SME using a generative AI application programming interface (API) to improve user experience could face higher costs, reduced access, or stricter contractual terms as the gatekeeper delays introduction of new features or withdraws marketplace management services in order to avoid liability. This would not only create legal and financial uncertainty for smaller companies, but also risk discouraging SMEs from adopting innovative AI technologies in the first place. Such an outcome would run counter to the DMA's objective of fostering competition and innovation in digital markets.

As one of our members stated, 'for a startup experimenting with location certification or proof of presence, AI being included as a CPS would freeze SME-led innovation." Giuseppe Tomei, Proxim.ai (Italy)

We therefore recommend caution to the European Commission when considering changes in the scope of the DMA. In the following section, we address the obligations established under the DMA on an article-by-article basis. We share our views on how these obligations apply in practice and their impact on SMEs and app developers.

### b. Obligations

Article 6

The DMA obliges gatekeepers to enable alternative app distribution channels, including third-party marketplaces and direct distribution via the web (Article 6.1-6.3). While this provision is intended to increase competition and user choice, our members have raised substantial concerns regarding its practical implications. For many SMEs, app stores do not merely function as distribution channels; they also provide a layer of intellectual property (IP) protection, consumer trust, and security assurance. Mandating the presence of distribution through alternative marketplaces on gatekeepers' platforms risks undermining these protections. Distribution options that are not designed to safeguard IP, privacy, or cybersecurity—such as the open internet—already exist, and our members choose gatekeeper platforms deliberately. Article 6 would undermine the enhanced protections they voluntarily seek in exchange for registration fees or commissions they pay to the designated gatekeepers' app stores. Our members fear that requiring the otherwise secure distribution channels to facilitate the spread of counterfeit or infringing applications degrades the more-secure options that, prior to Article 6's implementation, better enabled the protection of brand integrity and IP.

In addition, the proliferation of alternative distribution environments creates uncertainty around security standards and consumer protection. Smaller developers have faced increased costs and technical burdens in ensuring their applications remain secure across multiple, potentially fragmented ecosystems. This has disadvantaged SMEs relative to larger firms, which are better equipped to manage compliance and enforcement across diverse distribution platforms. 'As a small business, we don't have the resources to pay teams of lawyers to tackle long legal documents. So, my request to policymakers would be: please make compliance

simpler and easier for small businesses to interpret and implement.' Faizan Alam, REMODID (Austria)

We therefore urge the Commission to ensure that the implementation of Articles 6.1-3 is accompanied by robust safeguards for IP, consumer safety, and data protection.

To continue, Article 6 (4) of the DMA recommends allowing the 'installation and effective use of third-party software applications or software application stores' that may use or interoperate with the operating system of a gatekeeper. As most operating systems already allow third-party or 'sideloaded' apps and app stores, the aim of this article seems to be to make all app stores the same. However, there are valid reasons why a model that is more protective of the user experience may be preferable to a more open system. Significantly, several academic and industry sources have reported that in many cases open systems may face greater security challenges than more vertically integrated ones. A DMA that is too descriptive risks eliminating competitive differentiation, which could in turn reduce consumer choice and limit competition, outcomes that would directly contradict its objectives.

If the DMA only includes a narrow safeguard that lets gatekeepers protect system integrity but does not also consider user security, privacy, or data, it ends up favouring unrestricted third-party access and sideloading, even at the expense of consumer protection. Any measures taken to enhance interoperability must not come at the expense of security and privacy. Safeguarding these core principles is essential to maintaining consumer trust, which is the foundation of the app economy. Our members operate in an environment where consumers expect robust protections for their data and secure interactions with digital services. Therefore, we urge the Commission to ensure that proposed measures for interoperability align with established best practices for security and privacy. It is vital that interoperability frameworks do not introduce vulnerabilities or weaken the integrity of operating systems and connected devices.

Platforms play a crucial role in fostering consumer trust. By offering consumer protections such as secure payment systems, data privacy guarantees, and vetting processes for products and services, platforms create an environment where users feel more comfortable exploring offerings. This built-in consumer trust benefits all providers on the platform, but it is especially valuable for small businesses, which often lack the brand recognition and established reputation that bigger competitors enjoy.

In curated online marketplaces like app stores, one of the largest barriers to entry for small businesses is overcoming the network effects and brand loyalty enjoyed by more established players. In these highly competitive markets, platforms help smaller providers by giving them access to the trust and loyalty consumers have in the platform itself. This allows consumers to feel safer exploring products from less-established businesses, levelling the playing field and making it easier for small companies to thrive.

Moreover, besides security concerns, it remains unclear whether measures to create a fully open and interoperable app economy will in practice generate benefits for smaller actors. To date, our SME members have not experienced positive outcomes since the DMA came into force. 'The DMA is problematic for startups and SMEs like mine. Some provisions could break encryption and dismantle interoperability. As an SME, I can't afford that. When you cut

corners like this, it gets very dangerous for everyone.' Mitchel Volkering, vaic.at (located in the Netherlands)

Furthermore, Article 6 (3) of the DMA recommends that users be allowed 'to uninstall any pre-installed software applications' on a gatekeeper's core platform service if such an application is not essential to the functioning of the operating system or of the device. Some enforcement perspectives have gone further, arguing that all pre-installed apps should indeed be banned or that consumers should be presented with choice screens for every default app. We caution that such extensions go beyond the DMA's language and intent, and advocate for the Commission to refrain from expanding Article 6(3) beyond its intent.

With respect to Article 6(5), which prohibits gatekeepers from engaging in self-preferencing practices, we note that in general, self-preferencing, including by an online marketplace, is often pro-competitive. Marketplace management functions designed to bring consumers to the platform are both intended to attract individual consumers and lure in business users—they are examples of competition with other marketplaces that are also self-preferencing. However, we agree that self-preferencing can sometimes undermine fair competition. The Commission must not overestimate its DMA mandate in policing self-preferencing and be careful to preserve pro-competitive examples of it.

Regarding Article 6(7), we are deeply concerned that providing access without safeguards to a device's core features to business users and providers of services and hardware allows malicious third parties to reach sensitive device features. Bad actors could access cameras, contact lists, or virtual private networks without end-user permission, or track other devices in the same facility and hijack the functionality of other apps, risking end users' security and privacy. Our members rely on the safe environment that platforms provide to keep bad actors from accessing their app's data, while preserving consumer trust. This provision, thus, may unintentionally hurt them by making the app ecosystem less secure and decreasing consumer trust.

'The current enforcement of the Digital Markets Act is transforming digital markets in the EU into a homogeneous environment, eliminating choice for businesses like ours that focus on on-device, privacy-first approaches. Forcing curated platforms to design backdoors into operating systems in the name of interoperability is harming our business, driven by a fundamental misunderstanding of how consumer and business choice functions.' Mitchel Volkering, Vaic.at (located in the Netherlands)

Article 7

Article 7 of the DMA establishes obligations on gatekeepers to ensure interoperability of number-independent interpersonal communications services (such as messaging apps). Interoperability, while important, should never compromise data security, encryption, and privacy. Providers of messenger services of all sizes compete and differentiate themselves by offering stronger privacy protections, such as limiting data collection and restricting data sharing. Interoperability obligations risk eroding these competitive differences by forcing alignment with gatekeepers' standards. Moreover, achieving full interconnection generally requires the development of mirror features, common interfaces, and shared protocols, which can place a disproportionate burden on smaller providers.

In our view, this provision risks leading to a degree of product homogenisation, where messenger services converge around the same technical and functional baseline. Such convergence may ultimately reduce opportunities for differentiation and limit long-term innovation in this field. While we support the DMA's objective of enhancing user choice and contestability, it is essential that the implementation of Article 7 does not inadvertently undermine privacy-focused innovation or impose technical obligations that disadvantage SMEs.

Article 11

It's important that the compliance report template for designated gatekeepers reflects all relevant indicators, ensuring a comprehensive and transparent assessment of their obligations. In the following paragraphs, we outline the key elements that such reports should include to provide meaningful oversight and accountability.

Measuring the effect on app developers and innovation is essential, because SMEs depend on a variety of benefits offered by the app stores, including global distribution, increased consumer trust through curation, and protection from piracy. While these individual benefits may be difficult to measure, a decline in the number of SMEs offering apps, or in the revenues generated by SMEs through apps, would be a clear sign that there is something wrong and would require an adjustment in the way the DMA is implemented over time. Similarly, indirect effects on SME prospects such as increases in successful consumer fraud attempts and malware attacks are likely to indicate future problems for app developers, as consumers adopt a more sceptical approach to unknown software developers.

Additionally, a shift in app downloads and revenues towards larger app vendors would indicate that consumers have lost confidence that apps from unknown vendors won't be harmful. Several of the current curation processes go to great lengths to keep out bad actors. Platform payment systems also give consumers safety assurances by making it easy to get refunds or subscriptions. It is important that sideloading and alternate payment systems are implemented in such a way that warns and protects consumers from these bad actors. Otherwise, consumers will start only installing apps from well-known and trusted brands, which would be detrimental for SMEs and startups.

Platforms operate in two-sided markets, where designated gatekeepers compete for both end users and developers. When measuring the effectiveness of the DMA, it is important to measure the indicators of the *choices* rather than merely market share. For example, app makers decide which platforms to develop for based on a multitude of factors, including the availability of innovative operating system and hardware features, the potential target market, the availability of skilled talent, and the quality of development tools. What matters most is that app developers have choices, not necessarily which platform they ultimately choose to develop for.

Unfortunately, sideloading creates significant opportunities for bad actors to distribute pirated or hacked versions of apps. Precise measuring of the levels IP theft would indicate whether more protections and warnings for consumers are required. In addition, several vendor-specific app stores already have been extremely lax in their curation, resulting in an infestation of pirated content and malware. It is crucial that all app stores put strong measures in place to

combat piracy and IP theft. Piracy and malware not only reduce consumer confidence, they also cause a direct loss of revenues and can drive up costs for customer support, AI cloud services, and hosting related to pirated apps.

We believe measuring the effect of the DMA on consumers is equally important. We urge the Commission to closely track the prevalence of apps that include dark patterns, malware, and privacy violations. Much of this input for these indicators may already be available through monitoring of General Data Protection Regulation (GDPR) violations and complaints, as well as cybersecurity reports.

In addition to tracking direct harm to consumers, it would also be valuable to measure the confidence that consumers have to install unknown apps onto their devices. This may be reflected in actual downloads and app purchases, as well as through consumer surveys. General consumer confidence in apps is especially important for SMEs, who have enjoyed an increase in trust from the curation provided by the app stores.

Also, it is important to measure the level of competition and the choices available to consumers. The introduction of new hardware and operating capabilities, along with the competitive responses to new innovations are more indicative of competition than mere market share, which in itself may only indicate which choices offer the best product-market fit.

Lastly, measuring the effectiveness of the implementation and enforcement should be part of the compliance report. If complaints are handled with a focus that is too narrow and fails to consider the impact of potential remedies on the ecosystem, they may end up benefitting only a handful of companies, while causing more harm to many others. It is therefore important to involve all stakeholders in the evaluation of complaints and potential remedies. The loudest voices often don't reflect the most acute needs. Opposing interests within the ecosystem are common and should be considered.

Finally, it is of great value to measure how effective the processes in place function, including the steps such as correct data gathering, consultation of all stakeholders, and transparent decision-making. To ensure that the implementation of the DMA considers all stakeholders, it is important to measure indicators such as the participation in consultations, meetings, and workshops.

Article 15

We acknowledge the Commission's efforts to promote transparency in user profiling in order to preserve the trust of end users. We support encouraging competitors to differentiate themselves through the use of superior privacy guarantees. We agree that it is important for gatekeepers to be transparent with users about the information that is used to make decisions on what is offered.

With this in mind, we also want to highlight how certain profiling behaviours of app stores, such as in app recommendations, matching editorial content, and keyword-based search advertising, can benefit small and medium-sized app developers.

Today, app stores are filled with a great number of different kinds of products. Larger apps can attract new users through the strength of their existing brand, through the network effects of their existing user base, and the resources to run expansive marketing and advertising campaigns. Smaller apps rely on innovation and differentiation to build up their user base. Small app developers often gravitate towards niche app development that fills unexplored market gaps and opportunities. They identify specific needs or preferences that larger apps don't adequately fulfil. While this specialisation allows small developers to stand out in crowded app stores, opportunities for effective competition require access to a relevant dedicated user base. Smaller apps require app stores to use profiling techniques that can identify the users most likely to be interested in their specialised offerings.

App stores play a crucial role in developing editorial content that shows the benefits of apps for specific users. Especially for more specialised apps, it is essential that this editorial content can be shown to the most relevant users. While articles that spotlight specific apps may cater to a small audience, it is important to recognise that a select group of readers may possesses a profound level of interest and stands to gain immense value from the information presented. The apps featured in this content greatly benefit when app stores use profiling techniques to ensure they are shown to the appropriate target audience.

Finally, keyword-based search advertising is a powerful tool for small and medium app developers to reach new customers. Smaller app developers can efficiently increase the visibility of their apps using clearly marked, paid search ads that are shown to users searching for specific keywords. This enables precise targeting and cost-effective budget management for smaller businesses.

We support the Commission's objective to promote transparency in user profiling to continue to earn the trust of users. To foster a competitive environment for all participants of the app ecosystem, we ask the Commission to continue to preserve the ability for app stores to match niche apps with specific customers, using measured and transparent profiling.

### c. Enforcement

The enforcement of the DMA has so far been characterised by uncertainty and constant change. For SMEs, this has been particularly challenging. The frequent revisions to compliance plans by designated gatekeepers, often prompted by evolving interpretations from the European Commission of what compliance should entail, have not delivered tangible improvements for smaller businesses. Instead, these changes have introduced unpredictability into the ecosystem, leaving SMEs without the clarity and stability they need to plan and compete effectively.

Of further concern is the Commission's very limited of consultation with SMEs throughout the enforcement process. Our members, who are directly affected by both the obligations and the gatekeepers' responses to them, have not or only sporadically have been included in the dialogue. This undermines the objective of the DMA to create a fairer and more contestable digital market.

To ensure that SMEs and startups have a meaningful voice in the regulatory process, dedicated resources could be allocated within the DMA Taskforce to establish a consultative forum of

app developers. This forum would gather input from smaller players on market investigations, designation processes, and the practical effects of obligations on gatekeepers. This would help regulators understand the realities faced by SMEs and startups, ensuring that DMA enforcement is proportionate, innovation-friendly, and responsive to the needs of the broader ecosystem.

Unfortunately, enforcement has led to delays in the rollout of certain tools and technologies, including AI features,[2] which are critical for SMEs to remain competitive at the global level. Such delays leave our members at a disadvantage compared to peers in other regions where regulatory barriers have not slowed access to innovation. As stated by our member, 'when we develop breakthrough features like our COPD early detection tool with AstraZeneca or our professional dashboard for healthcare providers, platform approval delays can mean months where people who need help can't access it. Every friction point, whether it's scary alternative app store warnings or restrictive monetization policies, potentially costs lives.' - Geoffroy Kretz, Kwit (located in France).

Finally, we note the absence of a central, accessible resource where startups and developers can easily review and compare the compliance plans of all gatekeepers. As gatekeepers and the Commission negotiate over implementation of specific articles, compliance plans undergo iterative changes, and it has been difficult at times to identify which proposed compliance plans are most recent and which are viewed by the Commission as being most likely in compliance with the law. Having a single point of reference would enhance transparency, reduce information asymmetries, and allow SMEs, startups, and scaleups to better understand how gatekeeper obligations are being implemented in practice.

### d. Implementing Regulation and procedure

Article 6 of the DMA Implementing Regulation lays down the rules for the application of Article 34 of the DMA, specifically concerning the right to be heard and access to the file. Article 34 obliges the Commission to 'give the gatekeeper […] the opportunity of being heard on: (a) preliminary findings […] and (b) measures that the Commission may intend to take given the preliminary findings' and provides that gatekeepers may submit their observations to the Commission's preliminary findings within a time limit of at least 14 days. Opposed to these general provisions, Article 6 of the Implementing Regulation sets out strict rules for the application of Article 34. It only allows the gatekeeper (the 'addressee of the preliminary findings') to succinctly inform the Commission of its view in writing and submit evidence thereof.

Article 6 of the Implementing Regulation does not address the rights of third parties to be heard at all and severely limits both gatekeepers' and third parties' rights to be heard. Only allowing gatekeepers to submit 'succinct' observations to preliminary findings in a maximum of 50 pages, and even less for substantiated arguments as part of the gatekeeper designation process, seems overly prescriptive and given the complexity of the matter at hand, like an arbitrary page limit. We are concerned that with such stringent limitations, any broader perspective on the implications for all parties within the ecosystem, including and especially SMEs, will be

[2] https://www.reuters.com/technology/artificial-intelligence/apple-delay-launch-ai-powered-features-europe-blames-eu-tech-rules-2024-06-21/

omitted. In addition, Article 6 of the Implementing Regulation considerably limits the gatekeepers' and third parties' right to be heard, as it does not even foresee a right to be heard orally or mention the role of a Hearing Officer. In this context, we emphasise the disjointedness between the DMA Implementing Regulation and regular EU antitrust procedures, which guarantee an oral hearing.

While under EU competition rules, third parties (i.e. all natural or legal persons, undertakings, and associations of undertakings other than those under investigation [and other than the Commission and Member States' authorities]), also only have limited possibilities to express their views in pending proceedings, but at least these possibilities exist. Such possibilities include submitting comments to Commission press releases and website publications and providing comments on Commission market test notices, which always contain an explicit invitation for third parties to submit observations within a time limit of no less than one month.

Similarly, under general EU competition law, third parties have no right to the European Commission's investigation file. While the companies under investigation have a right to access this file, once the Commission has addressed to them a statement of objection, third parties cannot access it. Nonetheless, EU competition law foresees that third parties can strengthen their procedural position by requesting to be heard as an interested third person or party, provided they fulfil the requirements below:

- Article 27 (3) of Regulation 1/2003 on the implementation of the rules on competition provides that natural or legal persons who 'show sufficient interest' have a right to be heard.
- Recital 32 of the Regulation clarifies that a third party has 'a sufficient interest' when its 'interests may be affected by a decision'.
- Whereas complainants must show that '[their] economic interests have been harmed or are likely to be harmed' because of the alleged infringement of Articles 101 or 102 TFEU, interested third persons could either be harmed by the alleged infringement or benefit from it. Their interest in being heard may thus be either against or in support of the companies under investigation.
- While consumer associations that apply to be heard are generally regarded as having sufficient interest where the proceedings concern products or services used by the end consumer, business associations have sufficient interest if their members would individually have sufficient interest and the association is entitled to represent the interests of its members.
- Applications to be heard can be submitted from the date of the initiation of proceedings. The European Commission's independent competition Hearing Officer is in charge of granting the right to be heard to a third party if it is deemed to have sufficient interest.

If a third party is granted the right to be heard, the Commission must inform the third party in writing of the nature and subject matter of the procedure and must set a time limit within which the interested third party may make known its views in writing. If the interested third party requests so in its written comments, the Commission's Hearing Officer may, 'where appropriate', allow the interested third party to express their views also at the oral hearing of the parties to which a statement of objections has been issued.

Given the above, the App Association strongly encourages the Commission to align the DMA Implementing Procedures with EU competition law. The Commission should explicitly provide for the involvement of third parties in the DMA Implementing Regulation and the right to be heard by:

- Allowing third parties to submit written comments and to be heard on the file, under the same conditions as for competition law procedures (if they can show sufficient interest).
- Guaranteeing gatekeepers the possibility to be heard orally in the framework of the DMA, as is the case in EU antitrust investigations.
- Involving independent Commission antitrust Hearing Officers in all DMA procedures like in EU antitrust procedures, including concerning the possibility to grant interested third parties to be heard.
- Reviewing the page limits of Annex II to allow gatekeepers to reasonably make use of their right of defence.

Article 7 of the DMA Implementing Regulation concerns the identification and protection of confidential information. We welcome that third parties can request anonymity and that the Commission can restrict the means of access to information on which businesses have claimed confidentiality. Businesses of all sizes must be able to protect their sensitive information, especially SMEs that tend to be more vulnerable to risks from disclosing such information than larger companies. We appreciate the Commission explicitly asking companies that are submitting documents to identify such business secrets or other confidential information.

### e. Effectiveness and impact on startups and SMEs

To date, our members have not experienced tangible benefits from the DMA. Instead, they face increased uncertainty and additional difficulties in doing business, largely due to the constant changes in gatekeepers' compliance plans and the lack of a stable and predictable enforcement framework. Rather than reducing barriers, the DMA has so far introduced more complexity into the operating environment for smaller companies.

This concern is also reflected in Atomico's 2024 *State of European Tech* report, which surveyed 3,000 tech founders and investors. The findings show that 41 per cent are dissatisfied with the DMA, 38 per cent see no significant change, and only 22 per cent view it positively. This data underscores that the regulation is failing to deliver meaningful benefits for SME developers, reinforcing the need for a more measured and effective approach.

Member of the App Association' Clément Sauvage, Bits'n Coffee Consulting (located in France), said the following:'Does the DMA actually benefit European developers? History says no. The Epic vs Apple conflict has already damaged small developers badly: instability, blurred rules, and legal uncertainty. We became the battlefield, without asking for it. Now, the DMA risks replaying the same story on a European stage. And as always, it's the smaller ones who end up paying the bill.'

DMA has so far primarily benefitted established brands, while offering little to startups and SMEs. For young companies, what is needed above all is a trusted and predictable environment

in which to grow, innovate, and compete on fair terms. The reality, however, is that the DMA's current implementation has not provided this foundation.

Furthermore, a survey conducted by Nextrade Group among 5,000 European consumers found that, since the DMA took effect, most respondents report a decline in the quality and relevance of digital services. Two-thirds report having to spend up to 50 per cent more time searching for relevant information, and significant numbers note declines in the usefulness of map services (35 per cent ), search result relevance (33 per cent), and personalisation in job leads (25 per cent) and ads (39 per cent)[3]. While the DMA's intention was to empower users and startups, these findings suggest that instead, consumers and SMEs are confronting increased friction and degraded service quality.

## III. Conclusion

All in all, the experience of our member companies demonstrates that while the objectives of the Digital Markets Act are well-intentioned, its current implementation falls short of delivering meaningful benefits for SMEs and startups. Instead, it has introduced greater uncertainty, compliance fragmentation, and unintended barriers that threaten to undermine the innovation and contestability it aims to foster. To ensure that the DMA achieves its stated purpose, it is critical that enforcement mechanisms become more predictable, transparent, and inclusive of SME, startup, and scaleup perspectives. Only by involving all stakeholders, especially the smaller companies most dependent on fair access to digital platforms, can the Commission build an environment that sustains consumer trust, safeguards security, and allows innovation to flourish across the ecosystem.

Looking ahead, the App Association stands ready to collaborate with the Commission to refine both the framework and its enforcement. In particular, we believe that future reviews of the DMA should explicitly address the disproportionate burdens borne by SMEs, ensure robust safeguards for consumer security and privacy, and preserve the opportunities for smaller developers to compete on a level playing field.

Sincerely,

Mike Sax
Founder and Chairperson

Maria Goikoetxea
EU Policy Manager

Giulia Cereseto
EU Policy Associate

[3] https://www.nextradegroupllc.com/impact-of-the-dma-on-eu-consumers