4 December 2025

Feedback of

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

to the

European Commission and European Data Protection Board

regarding the

# Consultation on the Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation

## I. Introduction

ACT | The App Association (hereafter 'ACT') welcomes the opportunity to submit comments to the European Commission and European Data Protection Board's consultation on the joint guidelines on the interplay between the Digital Markets Act (DMA) and the General Data Protection Regulation (GDPR).

ACT 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 ACT 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]

## II. General Position

ACT welcomes clarity on the draft guidelines on the interplay between the DMA and the GDPR and supports efforts to ensure a safe, transparent, and privacy-respecting digital environment. As companies across Europe adapt to this evolving regulatory environment, clear and practical guidance will be essential to support privacy-preserving innovation, maintain strong security standards, and ensure predictable implementation.

While this consultation focuses on a limited set of DMA Articles, further clarity on additional Articles and cross-compliance scenarios would help reduce uncertainty and support a more coherent and user-protective framework overall. In particular, additional guidance on Article 6(7) would be valuable, as questions remain on how interoperability obligations can be implemented without compromising platform security or user data protection. Expanding on the privacy obligations relevant to similar provisions would help set compliance expectations and build solutions that uphold both privacy and competition goals.

## III. Article 6(4)

The clarification that Article 6(4) does not imply a joint controllership or controller-processor relationship is useful, as small and medium-sized enterprises (SMEs) lack the legal and operational resources of larger firms to interpret complex regulatory structures or absorb downstream effects of gatekeepers' compliance decisions. While SMEs remain responsible for their own processing activities, it is essential that the guidelines include guardrails that preclude shifting responsibility, liability, or operational burdens on smaller business users. Clear delineation of responsibilities helps ensure SMEs are not inadvertently exposed to expanded obligations or risks arising from implementation.

However, even with such guardrails and the security-focused measures outlined in the guidelines, Article 6(4)'s broad access obligations and the GDPR's requirements for informed,

[1] *See* https://actonline.org/wp-content/uploads/220912_ACT-App-EU-Report.pdf

controlled data processing create significant uncertainty for both SMEs and users who rely on predictable, trusted ecosystems. For example, the requirement that Article 6(4) beneficiaries receive sufficiently granular API access to operate an app or app store assumes benign behaviour. In reality, malicious actors seeking to install harmful or privacy-invasive software could exploit this access to bypass longstanding protections. While the guidelines propose safeguards, further consideration of practical implementation risks is needed, as no set of measures can fully mitigate the security and privacy risks inherent in mandating broad, third-party access to core system functions. A more balanced approach would limit third-party access in ways that preserve user trust, maintain ecosystem integrity, and reduce risks.

## IV. Article 6(9)

The guidelines' requirement that gatekeepers provide clear, comprehensive, and easy to understand documentation and data portability interfaces will help SMEs navigate complex technical environments more effectively. Ensuring that documentation is clear, practical, and designed for accessible use by third parties will support the DMA's data portability goals without overwhelming small developers.

However, the suggestion that gatekeepers should not assess third parties' past compliance with GDPR obligations may limit gatekeepers' ability to anticipate and mitigate risks before they materialise. While we understand the intent to avoid unnecessary barriers to data portability, past compliance can serve as a useful risk indicator. As portability inherently broadens the ecosystem of data recipients, even a single breach could erode user trust and hurt legitimate small businesses that depend on consumer confidence to compete. Repeated incidents involving irresponsible data handlers are likely to push consumers toward well-established brands that signal trust through scale and name recognition. This dynamic will disadvantage SMEs, which may struggle to prove reliability in a marketplace where a single data breach can destroy consumer confidence.

To prevent unintended harm to competition and user protection, the final guidelines should clarify how to effectively consider third-party compliance risks without creating barriers for SMEs seeking to access the ecosystem.

## V. Article 6(10)

ACT welcomes the guidelines' emphasis on ensuring data access documentation and related processes are clear, accessible, and easy for businesses and end users to understand. Maintaining this focus on usability is essential, as unnecessarily complex or overly technical documentation risks creating confusion and weakening compliance across the digital ecosystem.

However, the requirement for gatekeepers to provide mechanisms through which business users may obtain consent from end users would benefit from further clarification, particularly with respect to interface design. Consent mechanisms that meaningfully inform users of how their data will be used, accessed, and potentially combined can be difficult to design in practice. Without clear parameters, gatekeepers and SMEs may face uncertainty in ensuring that individuals whose data is shared have transparency into how their information is processed and by whom.

The guidelines should offer more practical guidance on how to maintain user-friendly interfaces. Consumers are likely to feel overwhelmed if faced with repetitive or poorly timed consent screens, leading to reflexive approval that undermines the purpose of informed consent. Providing examples of effective consent flows and interface patterns would advance compliance, preserve user trust, and minimise friction.

## VI. Article 6(11)

While Article 6(11)—ensuring that such data is truly anonymised—is constructive in theory, operationalising it is likely to prove challenging. To avoid unintended privacy consequences and maintain user trust, the final guidelines or an implementing act pursuant to Article 8(2) should provide more direction on appropriate safeguards.

## VII. Article 7

While the goal of interoperability under Article 7 is understandable, mandating cross-service communication risks significantly weakens encryption in practice. Even though the guidelines suggest that interoperability can be achieved without undermining encryption, real world implementation suggests that significant challenges remain. Any requirement that compels platforms to interface with external systems inevitably expands the attack surface and increases the number of points where security measures can fail.

Strong encryption is a cornerstone of online privacy and security. It enables consumers to communicate securely, protects the sensitive information of businesses and governments, and underpins trust in the digital economy. Moreover, it safeguards data in an era of increasing cyber threats and state-sponsored attacks. Weakening encryption, even indirectly, creates systemic vulnerabilities that malicious actors can exploit at scale. Once encryption is compromised, consumers who relied on its security may be left vulnerable to surveillance, interception, and unauthorised disclosure.

Given the central role encryption plays in safeguarding privacy, the guidelines should be revised to ensure that Article 7 does not require, incentivise, or indirectly result in the weakening of encryption. Interoperability should not come at the expense of safety, security, or consumers' fundamental right to privacy.

## VIII. Conclusion

ACT welcomes clarity on the interplay of the DMA and the GDPR and supports efforts to advance a safe, transparent, and user-centric digital ecosystem. We recognise the difficulty of reconciling these two frameworks, given DMA's broad and granular requirements to sideline privacy protections in favour of bolstering competitors. However, the final guidelines must strike the right balance between promoting competition and maintaining strong privacy, security, and encryption protections. We appreciate the opportunity to provide feedback and welcome continued engagement as the guidelines develop.

Sincerely,

Mike Sax
Founder and Chairperson