11 March 2026

Feedback of

ACT | The App Association
(Transparency Reg. # 72029513877-54)
Square de Meeûs 35,
1000 Brussels, Belgium

to the

European Commission

regarding its

Digital Fitness Check

I. Introduction

ACT | The App Association (ACT) welcomes the opportunity to submit comments to the European Commission's consultation on the Digital Fitness Check.

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 the European Commission's initiative to conduct a Digital Fitness Check and its broader commitment to simplify the EU digital regulatory environment. As outlined in the call for evidence, the objective of assessing complementarity, coherence, and cumulative impact of the EU digital rulebook is both timely and necessary. Moreover, both the Draghi[2] and Letta[3] reports constitute important analyses of how the accumulation of digital laws has a negative and adverse impact on the competitiveness and economic growth of European companies.

Over the last 10 years, the EU has adopted a comprehensive set of digital regulations and directives resulting in more than 100 texts, including the Artificial Intelligence Act (AI Act), the Digital Markets Act (DMA), the Digital Services Act (DSA), the Data Act, the General Data Protection Regulation (GDPR) and the Cyber Resilience Act (CRA).

The cumulative impact of these regulations is increased compliance complexity, with regulatory overlaps and enforcement fragmentation across EU Member States. This particularly affects small and medium-sized enterprises (SMEs) and startups.

Small companies are the backbone of the European economy and central to achieving the EU's competitiveness and innovation objectives. However, they still face disproportionate cost and time loss when they must comply with overlapping obligations and duplicative reporting requirements, while also facing compliance uncertainty. For smaller companies with limited legal and compliance resources, regulatory fragmentation quickly becomes a structural barrier to scaling within the Single Market.

'There are quite a lot of laws. It's a big barrier for small companies to innovate. You need to have lawyers; you need to apply some laws, and so on and so on. It's extremely challenging for small companies to compete with the big companies or small companies from other continents because there are too many complicated laws.' Sveatoslav Vizitiu, CEO, Rhuna.io

In this context, the Digital Fitness Check represents a timely opportunity to:

[1] See https://actonline.org/wp-content/uploads/220912_ACT-App-EU-Report.pdf
[2] https://commission.europa.eu/topics/competitiveness/draghi-report_en
[3] https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf

- Map and address overlapping documentation and reporting obligations;
- Align definitions and compliance timelines;
- Strengthen coherence and implementation between national and European authorities; and
- Ensure an innovation-friendly implementation remains proportionate to the risk and to the size of the company.

Simplification should focus on making compliance workable in practice, in particular for small innovators and companies, while preserving EU fundamental rights.

In particular, ACT encourages the Commission to:

- Establish a 'once-only' compliance principle, where documentation prepared to comply under one instrument can be reused for compliance under related frameworks.
- Harmonise incident-reporting timelines and formats across cybersecurity and data protection laws (e.g. GDPR and CRA).
- Establish a single reporting mechanism that satisfies multiple legal obligations simultaneously, on which companies can submit their compliance reports and documentation.
- Ensure that supervisory authorities, both at the national and European levels, are aligned to avoid inconsistent interpretation and application.
- Ensure a better alignment between the process of data under the AI Act and the GDPR.
- Provide guidance on the implementation of DMA obligations without compromising GDPR compliance.

III. Processing of data under the AI Act and GDPR

The interaction between the Artificial Intelligence Act and the General Data Protection Regulation is particularly relevant where AI systems involve the processing of personal data.

While Article 2(7) of the AI Act explicitly states that it is without prejudice to EU data protection law, the combined application of both frameworks creates practical complexity for organisations, especially small and medium-sized enterprises (SMEs).

The GDPR follows a horizontal and principle-based approach. It applies to all personal data processing activities, regardless of sector or technology, and requires that processing be lawful, fair, transparent, limited to specific purposes, and proportionate (Article 5 GDPR). Any use of personal data must rely on a valid legal basis under Article 6 GDPR, and where special categories of data are concerned, on an exemption under Article 9(2).

The AI Act, by contrast, regulates AI systems through a risk-based, product-safety logic.

However, where those systems process personal data, compliance with the GDPR remains fully applicable. In practice, this creates three main areas of friction in relation to data processing.

- First, the concept of 'high risk' is different between the two instruments. Under Article 35 GDPR, a Data Protection Impact Assessment is required where processing is likely to result in high risks to individuals' rights and freedoms. Under the AI Act, certain systems are formally classified as 'high-risk' based on predefined categories, establishing the need for a separate risk management and, in some cases, Fundamental Rights Impact Assessments. This may require organisations to conduct parallel assessments covering overlapping issues, increasing compliance burdens without necessarily improving protection outcomes.

- Second, the processing of special categories of data creates a compliance tension. Article 10(5) of the AI Act allows the use of sensitive data for bias monitoring and correction in high-risk systems, subject to safeguards. However, this provision does not create a standalone legal basis under Article 9 of the GDPR. Controllers must still identify a valid exemption, such as substantial public interest under Article 9(2)(g). As national approaches to this exemption may differ, organisations may face uncertainty when attempting to reconcile bias mitigation obligations under the AI Act with strict data protection constraints.

- Third, documentation and accountability requirements overlap. The GDPR requires records of processing activities (Article 30) and appropriate technical and organisational security measures (Article 32). The AI Act imposes logging, technical documentation, and traceability obligations for high-risk systems. While the objectives are aligned, SMEs may need to maintain parallel documentation structures to satisfy both regimes.

'We use AI a lot in our business, from marketing to sales, even drafting proposals. But a lot of the policies are unclear. As a small business, we don't have the resources to pay teams of lawyers to tackle long legal documents. A lot of things are unclear. For small businesses, we do not have a lot of resources to tackle all of these documentation requirements and translate them, and if you take them to the lawyers, it's a lot of extra cost.' Faizan Alam, CEO Remodid GMBH

Overall, the challenge is not a lack of legal safeguards, but the cumulative and partially misaligned application of two frameworks governing the same data processing activities from different regulatory perspectives. Greater alignment of risk assessment methodologies, clarification regarding special-category data, practical guidance, and coordinated supervision would improve legal certainty and reduce disproportionate burdens on startups and SMEs, while fully preserving fundamental rights protections.

IV. Regulatory overlaps between the DMA and the GDPR

The growing body of EU digital legislation has brought significant challenges also for competition and digital market regulations. In this context, the coexistence of the General Data Protection Regulation and the Digital Markets Act has introduced areas of regulatory overlap that can create uncertainty for businesses, particularly SMEs.

While both frameworks are designed to protect European consumer interests, their obligations sometimes intersect in ways that are unclear or operationally challenging. SMEs, which often lack the legal and technical resources of larger firms, are disproportionately affected by these ambiguities.

Certain DMA provisions, such as broad data access, interoperability requirements, and data portability obligations, can conflict or overlap with GDPR principles.

For instance, practical challenges remain between the implementation of Article 6(4) DMA and the GDPR. The DMA requires broad third-party access to certain platform functionalities, including granular API access. However, under the GDPR, any processing of personal data must be lawful, transparent, limited to what is necessary, and secure. Expanding access to core system functions may increase the volume of personal data shared and the number of actors processing it, making it more difficult to ensure compliance with data minimisation, purpose limitation, and security requirements.

This creates uncertainty for SMEs, which continue to grapple with the impacts of the Commission's DMA-related conduct mandates on the digital platforms that SMEs widely rely on. Across digital platforms, both those targeted by the DMA and those not designated as Gatekeepers, SMEs may either over-restrict access to avoid GDPR risks, thereby limiting competition and innovation, or over-share data to comply with DMA obligations, risking inadvertent privacy violations and as a consequence reduced trust in the ecosystem. Greater alignment and practical safeguards are therefore needed to prevent conflict between competition objectives and data protection rules.

The interplay between GDPR and the DMA also highlights tensions between competition and privacy objectives. The DMA aims to foster innovation and mandate open access and interoperability, while the GDPR prioritises robust protection of personal data and user control. In scenarios where data portability or interoperability expands the ecosystem of potential data recipients, businesses must carefully evaluate risks to ensure that user data is processed lawfully, transparently, and securely.

'The DMA raises some concerns to my business. Certain interoperability requirements, particularly for encrypted messaging services, create real compliance tensions that could

weaken end-to-end encryption protections in practice. As an SME, I worry about the downstream effects of this. While the DMA's obligations fall primarily on large gatekeeper platforms, the cascading impact of their compliance costs may ultimately be passed on to businesses like mine that depend on those platforms. This could lead to increased costs for my company and may ultimately force us to raise the pricing of our solutions, which would be bad for our business, our products, and consumers.' Mitchel Volkering, CEO, Vaic.at

Addressing these overlaps requires a coordinated approach that clarifies the boundaries between the two frameworks. Guidance should provide clear examples of how DMA obligations, such as interoperability or data access, can be implemented without compromising GDPR compliance. This could include specifying safe technical and organisational measures, risk assessment practices, and compliance guardrails that allow SMEs to meet both regulatory requirements efficiently. Harmonised rules would reduce duplication of effort, lower operational risks, and ensure that both privacy and competition goals are advanced coherently.

Additionally, the DMA unintentionally increases the risk of intellectual property infringements for SMEs by requiring gatekeepers to allow broad access to third-party app stores. Under the DMA, gatekeepers have limited ability to fully vet or monitor these external stores, which may host or facilitate content that infringes SMEs' proprietary software, algorithms, or other IP. As a result, SMEs face a heightened risk that their innovations could be copied, misused, or exploited without effective recourse. In the context of the EU's digital fitness check, this raises concerns that DMA obligations could weaken IP protections for SMEs unless stronger safeguards are implemented to mitigate these enforcement gaps.

In conclusion, the interaction between the GDPR and the DMA creates practical challenges that can hinder innovation, disproportionately affect SMEs, and generate legal uncertainty. The EU should prioritise developing detailed, SME-friendly guidance that aligns the two frameworks, clarifies responsibilities, and provides practical solutions for data access, portability, and interoperability. By doing so, policymakers can ensure that European businesses can compete effectively, leverage innovation responsibly, and uphold the highest standards of user privacy and trust in the digital economy.

Lastly, we urge the European Commission for a stable implementation of the DMA in order to allow startups, who rely on the established ecosystem, to develop their products the fastest and easiest way possible.

V. Incident reporting requirements

Under the EU digital rulebook, companies are required to comply with several reporting obligations that depend on the type of incident experienced and the regulators involved. This process also involves the use of different reporting forms, filled out with different information and with different deadlines under the NIS2, the Cyber Resilience Act, and the GDPR.

While these frameworks pursue the legitimate objectives of protecting users' data and ensuring cybersecurity resilience, their reporting obligations involve different timelines, formats, and competent authorities.

A single incident may therefore require multiple notifications within 24 or 72 hours to different regulators at both national and EU levels.

For SMEs, this creates significant operational issues at a moment when resources should be focused on remediation and communication with affected users. The absence of fully aligned one-stop-shop mechanisms creates more burdens, particularly for cross-border operators that must navigate different national procedures and language requirements. As a result, the cumulative reporting architecture risks prioritising procedural compliance over effective incident response.

For these reasons, ACT strongly supports the streamlining of reporting incidents into a single and EU-wide one-stop-shop mechanism, with harmonised timelines and procedures.

VI. Conclusion

The consultation on the Digital Fitness Check represents a key and valuable step toward addressing the cumulative effect and impact of the EU's digital regulatory framework.

While each digital framework serves an important purpose, their overlapping documentation requirements and inconsistent implementation across Member States generate legal uncertainty, increase compliance costs, and can unintentionally hinder innovation and market entry.

ACT welcomes the Commission initiative and purpose of simplifying the digital framework by addressing these challenges, clarifying interactions, harmonising definitions, and streamlining reporting and compliance processes. ACT urges policymakers to adopt a coordinated and SME-friendly approach that preserves high standards of data protection, privacy, and competition while making compliance workable in practice. By doing so, the EU can foster an environment where innovation thrives, SMEs scale within the Single Market, and citizens benefit from both robust privacy safeguards and competitive digital markets.

ACT stands ready to continue working with EU policymakers, bringing the voice of European SMEs and startups into the dialogue, and ensuring that the outcome of the Digital Fitness Check truly reflects the needs of those who are suffering more from compliance burdens.

Sincerely,

Mike Sax
Founder and Chairperson

Maria Goikoetxea Gomez de Segura
Policy Manager

Giulia Cereseto
Policy Associate