14 October 2025

Feedback of

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

to the

European Commission

regarding the

Consultation on the Digital Omnibus

## I. Introduction

ACT | The App Association (hereafter 'App Association') welcomes the opportunity to submit comments to the European Commission's consultation on the Digital package – Digital Omnibus.

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]

## II. Current challenges

The European Commission's 2025 Work Programme stated clearly that the focus will be on delivering *'bolder, simpler and faster'* regulatory landscape, closely aligned with the needs of European small businesses. In this regard, the App Association welcomes the Commission's effort in simplifying the current digital landscape to bring immediate administrative relief to businesses.

The EU digital rulebook has substantially increased in size and complexity during the last Commission mandate. Its rapid expansion with a high number of Regulations and Directives impacting the digital economy (e.g. the Digital Services Act, Digital Markets Act, Data Act, General Data Protection Regulation, ePrivacy Directive, and Artificial Intelligence Act) had a substantial effect on small and medium-sized enterprises (SMEs) and startups. As correctly stated by the European Commission in the call for evidence, compliance costs, reporting requirements, and unintended consequences scale disproportionately for smaller companies, undermining EU competitiveness.

We believe that simplification should be the driving cornerstone of the current mandate to ensure that competitiveness objectives are reached. As highlighted in the Draghi Report,[2] the current excessive regulatory and administrative burden is hindering EU companies from scaling and growth, producing a negative effect on productivity, leading in the last instance to deterring competition.

SMEs and startups are the backbone of the European economy, and, at the same time, they are the most affected by overlapping rules and fragmented enforcement, which have a direct impact on their capacity to work and on financing their businesses.

For these reasons, the Commission must prioritise simplifying the current EU legal framework, carefully evaluating new proposals, and enhancing implementation and enforcement of

[1] *See* https://actonline.org/wp-content/uploads/220912_ACT-App-EU-Report.pdf
[2] Mario Draghi (2024), Report on the future of European competitiveness, p. 317

existing rules in the Single Market to prevent overlapping legislation and redundant reporting obligations.

To achieve this goal and make the EU more competitive, the focus must shift to the specific needs of SMEs and startups. Streamlining their regulatory obligations and removing unnecessary administrative burdens will allow these businesses to innovate, scale, and compete more effectively within the Single Market and beyond.

## III. Harmonising risk management, documentation, and reporting requirements

SMEs across Europe face overlapping and disproportionate compliance obligations under multiple EU legislative acts.

Today, companies are simultaneously subject to reporting requirements under the General Data Protection Regulation (GDPR), Cyber Resilience Act (CRA), Data Act, and the ePrivacy Directive, and conformity assessments under the Artificial Intelligence (AI) Act.[3] Each framework imposes separate processes, timelines, and formats, resulting in duplication, fragmentation, and excessive compliance costs for small businesses.

Further, while reporting non-compliance carries substantial penalties, EU law does not give organisations adequate liability protection from regulatory action and/or civil litigation even when reporting requirements are fulfilled in the event of a cybersecurity attack. This dynamic creates an inherently adversarial compliance-based relationship between the Commission and companies, rather than a collaborative public-private partnership.

This regulatory complexity does not improve resilience. On the contrary, it drains resources and time from SMEs that could otherwise be invested in security improvements, innovation, and growth.

Incident reporting is a key example of this complexity.[4] Under the GDPR, CRA, and ePrivacy Directive, companies face multiple, often simultaneous, obligations to notify the same event to different authorities, within extremely tight timelines, and in different formats or languages. This overlaps only creates inefficiency and compliance cost, rather than improving security outcomes for citizens.

Moreover, it undermines EU ambitions and efforts to establish a truly integrated Single Market by requiring SMEs to file several reports on the same incident, sometimes within 24 - 72 hours, without the ability to rely on a one-stop-shop mechanism. This is particularly problematic for SMEs operating across several Member States, who may have to file identical reports in different national languages, to different regulators, and under diverging national processes. The lack of a centralised mechanism not only creates confusion but also increases the risk of inconsistent enforcement and legal uncertainty.

[3] Freshfields and DOT Europe (2025), Streamlining the EU Digital Rulebook.
[4] See above.

Simplification must therefore focus on alignment and consolidation of reporting and incident requirements. Specifically, small businesses should be able to access a simplified system for their reports, which should consist of:

- One-stop reporting: A single EU-wide reporting portal should cover all the reporting obligations under the EU digital law, such as the GDPR, and AI Act, and other relevant instruments. Reporting once should satisfy all obligations.

- Targeted mitigation of barriers to reporting: the EU should identify unnecessary barriers to timely incident reporting, such as liabilities organisations may take on through proactive information sharing, through appropriately scoped liability immunities or formal 'safe harbour' protections to organisations that report cybersecurity incidents or data breaches in good faith.

- Harmonised deadlines: Reporting timelines should be aligned across legislation, with clear rules on when the reporting time starts, to avoid conflicting requirements.

- Harmonised documentation: Risk assessments, technical files, and conformity documentation should be harmonised across different frameworks, in line with the Once Only principle.

Documentation requirements remain one of the most resource-intensive obligations for SMEs. A harmonised and proportionate regime is therefore critical to ensure compliance without deterring entrepreneurship or innovation.

Aligning risk management, documentation, and reporting obligations is not about lowering standards of security or fundamental rights protection. It is about making EU legislation work better for SMEs.

Simplification through harmonisation would reduce unnecessary burdens, increase legal certainty, and at the same time enhance both resilience and competitiveness in the European digital economy.

## IV. Ensuring a predictable and proportionate application of the AI Act

The App Association recognises the Artificial Intelligence Act as a cornerstone of the EU digital law to ensure a fair and safe use of the technology. We acknowledge the Commission's recognition that a smooth application of the AI Act is essential to ensure the competitiveness of Europe's digital economy.

Artificial intelligence systems are currently playing a critical role in driving innovation, improving productivity, and enabling SMEs and startups to scale in the global market. Particularly for small businesses, AI represents a transformative tool that can support growth and innovation, but only if the application is pursued in a clear, predictable, and proportionate regulatory environment.

Currently, however, companies face significant uncertainty. While many obligations under the AI Act are due to enter into force in 2026, essential guidelines, standards, and codes of practice

are still under development. Without these, businesses lack the clarity needed to comply with the requirements and adapt their products and services.

We therefore urge the Commission to consider pausing the implementation of the AI Act obligations until the regulatory landscape is clear and stabilised. As recently emphasised by stakeholder groups,[5] a two-year 'stop-the-clock' for the requirements would allow companies to prepare effectively to comply with the obligations, while also enabling the European institutions and the Member States to deliver on the necessary secondary legislation, guidelines, and supervisory board.

The delay of the implementation will not weaken the EU's commitment to foster trustworthy AI systems, but it will strengthen it by ensuring that obligations under the Act are implemented in practice, with a proportionate effort by SMEs and startups and consistent across Member States.

In the broader context of the Digital Omnibus and the forthcoming Digital Fitness Check on the legislative acquis in the digital policy area, this pause would create the necessary space to align the AI Act with other relevant legislation, such as the GDPR and the Data Act. It would also allow the Commission to identify other possible paths for simplification and ensure that SMEs can remain compliant without being deterred from adopting AI solutions.

Regarding the interplay between the AI Act and the GDPR, SMEs struggle with uncertainty around the processing of special categories of personal data.[6] While Article 10(5) of the AI Act allows such data to be processed for bias monitoring, detection, and correction in high-risk AI systems, this must still comply with the strict conditions of the GDPR, including explicit consent or substantial public interest grounds. This creates legal ambiguity, as organisations seeking to ensure non-discrimination may face conflicting obligations: the AI Act encourages the use of special categories of personal data to detect bias, while the GDPR limits its processing. Such uncertainty has practical consequences, as companies may be unsure whether they can lawfully process sensitive data to prevent discrimination without breaching data protection rules. Addressing this issue would help ensure that the AI Act's objectives of trustworthy and human-centric AI are met without infringing fundamental data protection rights. This tension is one reason why a temporary pause in the AI Act's implementation could be considered, to allow regulators and stakeholders to resolve these interpretative challenges and provide clear, harmonised rules.

Moreover, we encourage the Commission to take adequate measures to ensure that SMEs and startups are supported through the compliance processes without imposing other reporting requirements on them. In doing so, we welcome the AI Act's focus on limiting compliance costs, fees, and documentation for small businesses,[7] but we urge the Commission to work with Member States to ensure that this goal is reached and that they will deliver on the same level to ensure harmonisation across the EU.

[5] AI Champions Initiative
[6] EPRS, 2025, Algorithmic discrimination under the AI Act and the GDPR.
[7] AI Act, Recital 143

A simplified and innovation-friendly implementation strategy, based on clarity and proportionality, is the best way to ensure Europe's leadership in trustworthy AI while supporting the growth of its digital economy.

## V. Streamlining the Data Acquis

The App Association recognises the importance of Europe's data legislation in fostering trust, transparency, and responsible data sharing across the Single Market. These instruments play a central role in enabling data-driven innovation and ensuring that businesses and citizens can benefit from a secure and fair digital environment.

However, SMEs across Europe are also facing overlapping and simultaneous obligations under the Data Acquis. During recent years, the EU's data framework has evolved through multiple instruments, with overlapping provisions in the Data Act, Data Governance Act, the Open Data Directive, and the Free Flow of Non-Personal Data Regulation.

These instruments address similar issues but through separate rules, creating unnecessary complexity for businesses. This patchwork of rules leads to fragmentation, uncertainty, and substantial burden for businesses, especially SMEs and mid-caps that lack resources to manage complex compliance across regimes, hindering their competitiveness.

Data protection is a key cornerstone of EU law, but under recent studies,[8] the current framework is leading to a tension between different data protection instruments, in particular between the GDPR and the Data Act.

While the Data Act states that it operates 'without prejudice to' the GDPR and that the GDPR should prevail in case of conflict, in practice, companies struggle to interpret which rules apply in specific cases. The Freshfields analysis[9] found that businesses must often determine whether particular data is personal or non-personal and must reconcile diverging obligations under both regimes. In many cases, organisations may adopt conservative approaches by defaulting to full GDPR-level obligations to avoid legal risk, thereby increasing compliance costs and stifling data sharing.

To streamline this fragmentation, the Digital Omnibus should deliver better simplification by:

- Codifying and consolidating the data acquis into a single, streamlined framework that eliminates overlaps and clarifies responsibilities.
- Clarifying the interplay between GDPR and the Data Act, especially on data access and sharing, where conflicting obligations currently create uncertainty.
- Introducing SME-friendly exemptions to ensure proportionality and avoid applying the same requirements to micro-enterprises and large corporations.
- Modernising cookie rules to reduce consent fatigue, aligning ePrivacy Directive with GDPR, and providing businesses with clear and workable obligations while maintaining strong user protection.

By simplifying and consolidating the data acquis, the EU can reduce compliance costs, create legal certainty, and foster greater use of data-driven innovation.

[8] Freshfields (2024), When GDPR and Data Act clash: what Businesses need to know.
[9] See above.

## VI. Simplifying the European Digital Identity framework

The App Association welcomes the Commission's recognition that the European Digital Identity (EUDI) framework, including the forthcoming EU Business Wallet, represents a key instrument to enable secure and efficient digital business interactions.

As stressed above and correctly recognised in the call for evidence, SMEs and startups are currently facing high compliance costs and reporting requirements. We therefore believe that, also in the context of the revision of the EUDI framework, priority should be given to the simplification of procedures. Simplification should focus on reducing compliance costs and legal uncertainty while maintaining high standards of security and trust.

SMEs often face disproportionate obligations when interacting with multiple EU and national digital identity systems. A single, centralised portal for digital identity registration, authentication, and reporting would allow businesses to comply once, reducing duplication, administrative costs, and delays, particularly for cross-border operations.

As mentioned, it is therefore important that, in the context of the revision, priority should be given to the alignment with current EU legislation. The EUDI framework should be harmonised with GDPR, eIDAS, and other relevant legislation to avoid duplicative obligations. We therefore welcome the Commission's alignment with the 'one in, one out' principle; removing outdated or redundant requirements when introducing new obligations is vital to eliminate unnecessary regulatory burdens and ensure a predictable and proportionate environment for SMEs.

Moreover, the upcoming EU Business Wallet should integrate smoothly with existing business systems, be easy to use, and allow secure cross-border interactions. Technical complexity should not create a barrier to compliance, and smooth operation across Member States should reduce administrative costs while promoting digital innovation.

However, simplification should not undermine the protection of privacy and security. Reducing administrative burdens and legal complexity must never come at the expense of strong safeguards for personal data and user trust. The EUDI framework should ensure that privacy and security requirements remain robust, clear, and consistently enforced, so that businesses can simplify processes confidently without undermining the protection of citizens or the reliability of digital identity systems.

These measures will enable the EU Digital Identity framework to be truly SME-friendly, innovation-supportive, and harmonised, reducing unnecessary administrative burdens and legal ambiguity, while strengthening trust and cross-border interoperability.

## VII. Filter new proposals and better enforce current legislation

The App Association urges the European Commission to adopt a more strategic and proportionate approach to digital policymaking. Before advancing any new legislative initiatives, it is essential to carry out a deep assessment of the existing acquis to determine whether current instruments are fit for purpose, and where implementation or enforcement gaps may persist. The digital regulatory landscape has expanded significantly in recent years, often resulting in overlapping or even conflicting obligations. This creates costly compliance burdens, particularly for SMEs and startups, which lack the administrative capacity and resources to manage duplicative reporting requirements and fragmented rules across different frameworks.

We therefore encourage the Commission to prioritise effective enforcement, consistent interpretation, and targeted guidance over the introduction of new regulatory layers. A focus on maximising the impact of the existing acquis would reduce unnecessary complexity, enhance legal certainty, and provide businesses with the stability they need to invest and innovate in Europe.

In this context, we welcome the Commission's upcoming Digital Fitness Check on the legislative acquis in the digital policy area as a critical and timely exercise. By identifying where instruments collide, where obligations overlap, and where simplification is possible, the Commission can ensure that Europe's regulatory framework supports, rather than hinders, the competitiveness of its digital economy.

As part of this exercise, it will be crucial for the Digital Fitness Check to assess the cumulative impact of existing and upcoming digital regulations on SMEs and startups. Given their limited resources, smaller companies are disproportionately affected by fragmented compliance requirements and legal uncertainty. Integrating an SME impact assessment into the Digital Fitness Check would ensure that the regulatory framework remains innovation-friendly, proportionate, and aligned with the needs of Europe's digital entrepreneurs.

We strongly recommend that the findings of this process be used as a foundation to strengthen coherence and enforcement before considering additional legislation. This approach would avoid regulatory duplication, improve the functioning of the internal market, and create a more enabling environment for Europe's app developers and digital SMEs.

## VIII. Conclusion

The App Association welcomes the Commission's effort to establish a simplified legal framework in the digital law. As delivering a '*bolder, simpler, and faster'* Union is the core of the current Commission Work Programme, the simplification agenda must be the key pillar to deliver a consistent and coherent regulatory framework that avoids overlaps and inconsistencies between different pieces of legislation.

The Digital Omnibus represents a timely and unique opportunity for the European Commission to deliver on its promise and to help European companies to foster their growth in the EU market and beyond.

Simplification is not about weakening protection, but it is about ensuring that rules work for all companies, especially for small companies, which are the backbone of our economy, and are the ones who most need guidance in navigating the regulatory landscape and harmonisation.

In this view, the priority should be to:

- Ensure coherence and streamline among reporting requirements and documentation obligations;
- Ensure consistency of data and privacy rules;
- Pause the AI Act enforcement until the necessary guidance and structures are in place;
- Simplify the European Digital Identity Framework while ensuring strong protection of privacy and security;
- Filter and assess new legislative proposals.

Taken together, these measures will reduce compliance costs, unlock innovation, and strengthen Europe's competitiveness in the global digital economy.

The Digital Omnibus and the forthcoming Digital Fitness Check on the legislative acquis in the digital policy area can harmonise Europe's regulatory framework in a coherent, proportionate, and supportive way, ensuring that Europe's digital economy continues to thrive and grow.

Sincerely,

Mike Sax
Founder and Chairperson

Maria Goikoetxea Gomez de Segura
EU Policy Manager

Giulia Cereseto
EU Policy Associate