3 February 2026

Feedback of

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

to the

European Commission

regarding the

# Towards European open digital ecosystems

## I. Introduction

ACT | The App Association (hereafter 'ACT') welcomes the opportunity to submit comments to the European Commission's consultation on the European open digital ecosystems initiative.

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. Feedback on the European open digital ecosystems initiative

1. What are the strengths and weaknesses of the EU open-source sector? What are the main barriers that hamper (i) adoption and maintenance of high-quality and secure open source; and (ii) sustainable contributions to open-source communities?

Open-source software (OSS), defined by its publicly accessible and modifiable source code, underpins a substantial share of the digital infrastructure used by European SMEs, startups, and scaleups. From operating systems and cloud-native tooling to semiconductor design flows and artificial intelligence (AI) frameworks, OSS enables smaller firms to customise, develop, deploy, and iterate technologies that would otherwise require prohibitive upfront investment.

A core strength of the EU open-source ecosystem lies in its ability to lower barriers to entry and experimentation. SMEs and startups can access state-of-the-art technologies' up-front licensing fees, allowing entrepreneurs to focus on product differentiation, talent, and market entry. This is especially relevant in the early stages of company formation, where technology and cost decisions can determine long-term viability. Empirical research indicates that active engagement with open-source communities is associated with a significantly higher likelihood of attracting external investment, concretely, 36 per cent higher chances of getting investment, reflecting both improved technical credibility and stronger integration into innovation networks.[2]

At the same time, the EU open-source sector exhibits structural weaknesses that disproportionately affect SMEs. Many widely-used OSS components are maintained by

[1] *See* https://actonline.org/wp-content/uploads/220912_ACT-App-EU-Report.pdf
[2] https://pubsonline.informs.org/doi/epdf/10.1287/orsc.2023.18348

small teams or individual developers with limited and unstable funding, and there is limited strategic recognition at the leadership level of many organisations. This creates challenges for long-term maintenance, timely security updates, and formal assurance processes, despite the critical role these components play in commercial products and public infrastructure. SMEs that rely on such components often lack the resources to independently maintain or harden them, increasing systemic risk.

Legal and governance complexity is another significant barrier. SMEs frequently lack in-house legal expertise to fully assess open-source licensing obligations, particularly in cases involving copyleft licenses or complex dependency chains. Inadvertent non-compliance can expose firms to litigation risk or force disclosure of proprietary code, which is particularly problematic in digital markets where traditional IP protection mechanisms, such as patents, may offer limited practical protection. As a result, some SMEs adopt a risk-averse approach and avoid certain OSS components altogether, even where they would otherwise be technically optimal.

Finally, while open source enables rapid development, it can also complicate value capture for SMEs. When competitors can access the same open-source foundations, differentiation must occur at higher layers of the stack, such as services, integration, or data. Without supportive market conditions and clear regulatory frameworks, SMEs may struggle to convert technical innovation into sustainable commercial advantage, reducing their ability to contribute back to open-source communities over time.

2. What is the added value of open source for the public and private sectors? Please provide concrete examples, including the factors (such as cost, risk, lock-in, security, innovation, among others) that are most important to assess the added value.

For both, public administrations and private-sector SMEs, the added value of open source lies primarily in its impact on cost structures, flexibility, and long-term risk management. Open source can also mitigate the risk of vendor lock-in, which is a critical consideration for public-sector digital infrastructure and SME-led innovation alike.

From a security and trust perspective, while open source does not automatically guarantee security, its openness enables robust assurance processes when combined with appropriate governance and funding. In innovation-intensive sectors such as AI, cloud computing, and cybersecurity, open-source frameworks and toolchains have become widely used, allowing SMEs to compete on functionality and performance rather than on access to proprietary platforms.

Linux stands as a leading example of beneficial open-source software because its collaborative, community-driven development model, spanning thousands of contributors worldwide, has produced a secure, stable, and customisable operating system kernel that powers the majority of the world's servers, supercomputers, cloud infrastructure, smartphones (via Android), and embedded devices, all without reliance on any single proprietary vendor.

3. What concrete measures and actions may be taken at EU level to support the development and growth of the EU open-source sector and contribute to the EU's technological sovereignty and cybersecurity agenda?

To effectively support the development of the EU open-source sector and strengthen Europe's technological sovereignty, EU action should focus on enabling sustainable participation by SMEs and startups, which form the backbone of Europe's digital innovation ecosystem. Open source already underpins a significant share of Europe's digital infrastructure, yet its long-term sustainability can remain fragile due to underinvestment, fragmented support mechanisms, and regulatory frameworks that were not designed with open, collaborative development models in mind. Addressing these structural challenges is essential if open source is to fulfil its potential as a driver of competitiveness, resilience, and innovation.

From an investment perspective, the EU could place greater emphasis on funding the maintenance, security, and long-term viability of critical open-source components, not only the creation of new projects. Many of the most widely used open-source technologies are maintained by small teams or individual developers with limited financial resources, despite being embedded in commercial products and public infrastructure across Europe.

Access to capital remains a structural barrier for startups and small companies building on open-source business models. Unlike traditional proprietary software firms, open-source-based companies often generate value through services, integration, or complementary products rather than licensing revenue, which can make them less attractive to conventional investors. EU funding instruments and innovation programmes should therefore explicitly accommodate and support open-source-based commercial models, ensuring that eligibility criteria and evaluation metrics do not implicitly favour proprietary approaches. Policies should aim to preserve flexibility, lower barriers to entry, and enable startups to scale without being locked into specific technological or commercial models.

In the area of security and privacy, EU action should focus on strengthening the resilience of open-source ecosystems while avoiding disproportionate obligations that could discourage participation. Open source plays a central role in Europe's cybersecurity landscape, providing transparency, auditability, and rapid vulnerability detection. However, imposing product-level compliance obligations on volunteer-driven or SME-led open-source projects may risk undermining the very ecosystems that European industry relies upon. A more effective approach would be to support coordinated vulnerability disclosure, shared security tooling, and voluntary certification or assurance mechanisms that scale with the size and role of the actor involved.

Finally, EU action should promote coherence across digital policy initiatives to ensure that open-source development is not inadvertently constrained by overlapping or inconsistent regulatory requirements. Clear guidance on liability, licensing compatibility, and security responsibilities would significantly reduce legal uncertainty for SMEs and encourage broader participation in open digital ecosystems. By aligning investment, access to capital, and security policy with the realities of open-source development, the EU can strengthen its technological sovereignty while enabling startups and small businesses to innovate, compete, and grow within a truly open digital economy.

## 4. What technology areas should be prioritised and why?

Building and using technologies developed in open standard-setting organisations (SSOs), our members drive the EU's global internet of things (IoT) leadership by creating products and services that consumers across the European economy enjoy, and thrive in a transparent, competitive, and fair licensing environment. Priority should be given to technology areas where open source is both foundational and strategically relevant to EU competitiveness, and where SMEs play a central role as innovators and implementers. Standards-based technologies that rely on standard-essential patents (SEPs) are a particularly important example. SMEs increasingly implement technical standards through open-source software, and while some SSOs have moved to allow or encourage royalty-free licensing for standards important to open-source ecosystems, a lack of transparency around SEP licensing and abuse by a handful of SEP holders creates legal and financial risk that can deter market entry. Ensuring transparent, predictable, and genuinely fair, reasonable, and non-discriminatory (FRAND) licenses for all to SEPs is therefore essential for enabling SME participation and for aligning standards policy with open digital ecosystems. The Commission should recognise royalty-free SSO policies as one form of the FRAND licensing framework that may be selected.

## 5. In what sectors could an increased use of open source lead to increased competitiveness and cyber resilience?

Open-source technologies have the potential to enhance both competitiveness and cyber resilience across multiple sectors, particularly those that are standards-driven, innovation-intensive, or foundational to Europe's digital economy. In sectors reliant on SEPs, for example, royalty-free approaches to technical standards can significantly lower entry barriers for SMEs and startups, enabling them to develop interoperable products without facing prohibitive licensing costs or legal uncertainty. By facilitating access to essential technologies, such an approach fosters a more competitive market environment in which small developers can innovate alongside established players, contributing to overall ecosystem dynamism and European technological sovereignty.

In the artificial intelligence sector, open-source frameworks and models play an important role in innovation, experimentation, and reproducibility, particularly for startups and SMEs that cannot afford the infrastructure and licensing fees of proprietary solutions. Open-source AI components enhance cyber resilience by providing transparency, enabling peer review, and accelerating the detection and remediation of vulnerabilities. However, regulatory initiatives such as the Cyber Resilience Act, if applied without nuance, risk restricting access to open-source components or imposing compliance obligations that are disproportionate for small-scale contributors. This could inadvertently undermine both innovation and security in the AI sector, reducing the availability of shared tools that startups rely on to compete and scale.

More broadly, open source supports cyber resilience and competitiveness in public administration, cloud infrastructure, telecommunications, and internet of things applications. By providing transparent, interoperable, and auditable building blocks, open-source technologies reduce dependency on single vendors, lower operational risk, and empower SMEs to participate in sectors that are increasingly digital and interconnected. Ensuring that open-source ecosystems remain accessible, well-maintained, and appropriately supported is therefore essential to unlocking their full potential in strengthening Europe's digital economy while safeguarding security and resilience.

ACT remains committed to work together with the European Commission towards a more competitive and innovation-friendly Europe.

Sincerely,

Mike Sax
Founder and Chairperson

Maria Goikoetxea
EU Policy Manager

Giulia Cereseto
EU Policy Associate