Response to the European Commission Call for Evidence 2026
"Towards European Open Digital Ecosystems"

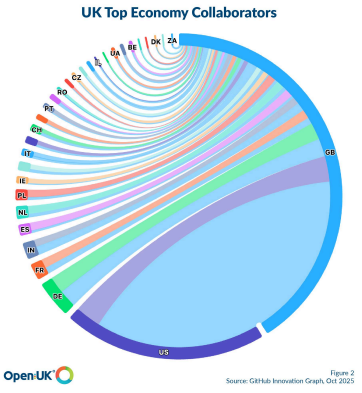
Submitted by: OpenUK, Legal Advisory Board
Country: UK
Respondent type: Non-profit organisation
Date: 3 February 2026
Contact: mailto:admin@openuk.uk

Summary
OpenUK welcomes the EU's consultation and the opportunity to make this contribution to the Commission's proposed strategic approach to the EU's Open Digital Ecosystem. We strongly support measures that: (1) fund and maintain foundational open source infrastructure; (2) reduce fragmentation and unlock interoperability; (3) strengthen security and resilience across sectors; and (4) enable global collaboration (including structured participation by non-EU partners such as the UK) to accelerate innovation.

The objectives are worthy, heading in the right direction, but key to these being successful is how the implementation of any strategy is achieved. We recognise decades of engagement across Europe have failed to see appropriate measures implemented to ensure a healthy ecosystem in which any European nation benefits, appropriately participates in and contributes back to the open source ecosystem, despite steps in the right direction.

Others in the EU are submitting detailed lists of these responses and we believe it would be inappropriate for OpenUK to suggest these, but OpenUK supports these and is currently working in the UK with our national funding body on similar and aligned recommendations.

EU projects benefit from extensive contributions from the global open source community/ Over 90% of today's software infrastructure having open source dependencies and over 70% of that being open source.



This open source software underlying all stacks in 2026 is dependent on open source from global contributors including from the UK. The UK continues to be Europe's leading contributor to open source software and 5th globally with significant collaboration with EU partners including in particular Germany and France who are the UK's second and third strongest collaboration partners.

The EU's approach to open source software is therefore not only relevant to EU countries and open source in those countries, but is of great significance to the UK and other global countries which engage in open source collaboration.

For the EU's approach to succeed to its potential requires a clear pathway to ongoing collaboration and an understanding that code created on an open-source-basis will benefit all nations in the same way as code from all nations underpins today's infrastructure and is available to the EU under open source licensing. Licensing is subject to local laws and this availability is subject only to a few specified exceptions due to export control and sanctions along with any local laws.

OpenUK encourages an EU policy that welcomes and organises its international collaborative efforts. We hope to enhance strong and engaged collaboration with the EU open source technical, governance, and policy communities.

Sovereignty is a key discussion globally and in particular for the EU. The role of open source in software, hardware, data AI and the future of innovation and the access to the technology open source enables is a cornerstone to creating sovereignty by enabling the removal of dependency on entities from any country. However it must be recognised that whilst this may be achieved through open source this is global open source and not "local source" initiatives.

Utilisation of existing code, innovation and AI allows the EU to stand on the shoulders of giants and strengthens the basis of EU digital sovereignty across its digital environments, this must recognise the global interactions at the heart of open source and also requires outputs to be globally available. Open source will enable the EU to grow shared capabilities, participate in the best innovation and reduce single points of failure, if this collaborative approach and a holistic view to funding, contribution and management is applied.

Policy options that ring-fence collaboration by geography or take a "go it alone" approach to digital, risk undercutting collaboration and will inevitably impact significantly Europe's competitiveness in the global economy; and ability to engage in and benefit from open source. We encourage both global collaboration as a starting point and a limited use of sanctions and other restrictions on global collaboration.

Specific Questions

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?

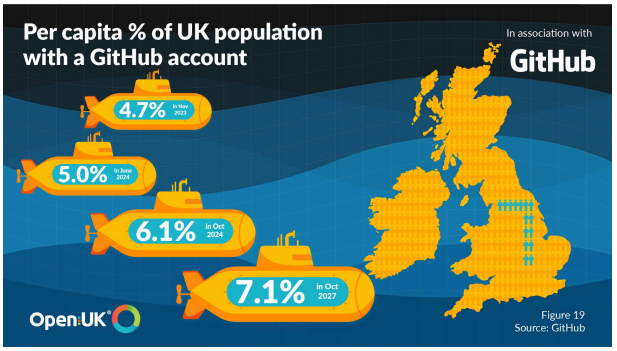
The EU benefits from a strong open source ecosystem, with Germany and France in particular showing strength in numbers of developers and projects hosted. Germany is currently seen to be 7th globally and whilst France has Europe's fastest growing open source community[1].

The EU's significant and active talent base reflects both scale and depth of capability, making enormous contributions to global open source development. This demonstrates a vibrant, productive ecosystem and confirms open source as a major pillar of European competitiveness and digital capacity.The success of EU open source is inseparable from wider international collaboration. Open source development is inherently transnational and EU projects routinely rely on contributions from elsewhere.

According to figures from GitHub[2], in 2025 – EU based open source projects received more than 553,000 code contributions from developers in the United Kingdom, highlighting the continued material role of UK expertise in the growth and health of European open source.

Any policy that creates barriers to such cross-border collaboration on open source would limit the diversity, sustainability and pace of innovation in the EU ecosystem. Open source communities thrive on global contribution flows, and the EU's strategy should aim to preserve and strengthen these links, including with close partners such as the UK.

Our research illustrates the scale of the UK's contribution. Using conservative estimates based on GitHub developer account data, the UK had around 109,460 accounts in 2018, increasing to approximately 126,000 in 2019 following typical growth rates. Today the UK has 4.8m GitHub accounts.



[1]https://github.blog/news-insights/octoverse/octoverse-a-new-developer-joins-github-every-second-as-ai-leads-typescript-to-1/#h-where-the-world-codes-in-2025

[2] GitHub Innovation Graph

When applying the European Commission's 2021 methodology for calculating economic impact, the UK's developer base represents an estimated £29.52 billion to £43.15 billion in economic value. This underscores not only the UK's strong skills base in areas such as cloud engineering, security, and open source compliance. Despite our obvious existing collaboration there is significant value in greater coordinated EU-UK collaboration which could deliver significant benefits to both EU and UK ecosystems.

Notwithstanding its strengths, the EU open source sector faces several challenges and barriers today Fragmentation across Member States continues to limit the effectiveness of large scale initiatives, leading to duplication of effort and inconsistent outcomes. Interoperability challenges remain a major obstacle.

Limited access to essential technical standards, coupled with high costs of standards, challenges in the use of Standard Essential Patents and licensing restrictions, create difficulties for open communities seeking to implement, verify or comply with standards.

In addition, skills shortages persist in areas that are critical to secure and sustainable open source development coupled with talent flight. Areas such as cloud orchestration, cybersecurity and governance whilst weak in the EU are comparatively strong in the UK and collaboration would be particularly beneficial for the EU.

Sustainable contributions to open source from the EU are also hindered by the absence of long-term funding mechanisms. Many foundational components that underpin European industry rely heavily on global volunteer labour or underfunded maintainers. Existing EU funding programmes tend to prioritise research and the development of new features, rather than providing the consistent and long-term maintenance, security hardening and infrastructure support that these critical components require. A significant shift will be required forfeiting up to 20% of that funding for maintenance if success is to be attained.

The EU, like the UK, has suffered from talent flight and a long history of open source success stories in business leaving Europe to flourish in the US, exemplified in critical projects like France's Docker.

In summary, the EU's open source sector has significant strengths, including scale, talent and productivity. However, fragmentation, interoperability barriers, skills shortages and funding sustainability all remain key challenges. Given the global nature of open source development, any restriction on cross border collaboration would exacerbate these weaknesses. A successful future EU strategy will therefore require a strong emphasis on international cooperation, including close partnership with the UK, alongside targeted action to address internal structural challenges and ensure the long-term health of the ecosystem.

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.

Open source creates significant economic, social and operational value across both the public and private sectors. In both the public and private sector. The benefits of open source include: (1) reduction in costs as no royalty licence fees; (2) remove costs through collaborative innovation; (3) benefit from third party and community contributions; (4) enable collaborative research and development; (5) improved deliverables; (6) accelerate delivery time; (7) increased agility in development process; (8) ability to re-cycle and re-use code; (9) improved understanding of good practices and governance; (10) engagement and connection; (11) building skills; (12) enabling collaborative research and development; (13) increased security; (14) trust through transparency; and (15) development of skills and Know-How. These advantages compound when foundational components are maintained as part of public digital infrastructure and digital goods and when standards and data are open and accessible for broad reuse.

Organisations have the potential to avoid vendor lock-in as they can access, inspect and adapt source code. In true open source models users may switch providers benefiting from interoperability, or fork projects where necessary. The benefits of open source removing lock-in can be reduced however by the service provider's use of a closed service layer, charges like egress fees and add-on proprietary code. As with many aspects of open source the key is in the how - meaning how the code, strategy or policy is implemented.

For creators of open source it offers the opportunity of unprecedented adoption in its go to market strategy and enables the creation of de facto standards like Linux and Kubernetes. Its fundamental premise of access and sharing sits at the heart of the free flow of its licensing, relying on the ability of anyone to use the code for any purpose. This in turn enables iterative global development. These principles have been exemplified in AI with the US-based Llama LLM being distilled alongside China-based Qwen to enable the creation of DeepSeek's R1 open model, improving AI innovation and reducing the cost of creating an LLM from $100m to $5m.

It was evident in that report that 100% of all start ups founded in the preceding three years used open source. It was also clear that more mature organisations planned to increase their investment in open source. Through the open source maturity cycle greater value is attached to skills development, collaboration, community participation and knowledge sharing as leading benefits of open source, ahead of direct cost savings. Yet direct cost savings are critical and cannot be ignored.

It is notable in our research that whilst cost saving is regularly the single most important reason for organisational use of open source software, the single biggest complaint is also cost. This recognises the dichotomy that although open source is royalty free it is not free, and has significant costs to be well managed. These costs are not surfaced in the same manner as in the traditional software environment and manifest in costs like conference engagement, membership fees and travel budgets to enable ecosystem engagement and build, as well as contribution to project and maintainer costs. For the EU to engage appropriately and fully, significant budgets are required. The nuance and complexity is yet

greater when it is understood that nation states' economic contributions to open source cannot succeed in isolation and must be achieved in a joined-up manner

Open source not only enables iterative innovation but accelerates product development cycles, and improves resilience. These factors explain why many businesses depend heavily on open source as the basis of the public cloud, databases, software tooling and operating systems. Today open source forms the basis of our national digital infrastructure.

Evidence from OpenUK's 2023 State of Open Report underlines the economic significance of these benefits to the UK by way of example. Open source contributed an estimated £13.59 billion in Gross Value Add (GVA) to the United Kingdom in 2022, representing approximately 27% of the UK's tech sector economy. This focus on the value generated by open source as opposed to cost of replacement was ground breaking and relevant to all seeking to understand the importance of open source. Similar data would be found for leading EU countries.

The success of open source and reaping its benefits is restricted by how it is implemented and how ecosystems are supported at a national level.

Historically open source was used by public sectors in particular to: (1) remove vendor lock-in and create interoperability; and (2) create publicly-funded code that was recycled and re-used. In recent times we have seen a third strength, its ability to generate influence through adoption added to this. In the public sector, open source aligns naturally with principles of openness, transparency, and accountability. Governments benefit from the ability to inspect and adapt software, which improves security assurance and reduces procurement risks. Open source adoption also fosters internal capability development. Civil servants can contribute to open source communities, learn new technical skills and engage directly with global development practices. Open technologies further support public sector mandates for transparent and auditable systems, which is particularly important in areas such as digital identity, public registries, welfare systems and public data platforms.

At the same time, the value of open source will be amplified when foundational components which are in effect public infrastructure are recognised and supported as digital public goods. Reliable investment in maintenance, security and long-term stewardship ensures that widely used libraries, packages and core tools remain secure and robust. The benefits of open source are also greatest when technical standards and public sector datasets are accessible on open terms, since this promotes interoperability, competition and innovation.

Across both public and private sectors, open source strengthens cyber resilience. Community driven development enables early detection and remediation of vulnerabilities, while forkability ensures that organisations can maintain operational continuity even if a supplier fails or a vulnerability is discovered in a core dependency. Open source also contributes to national and regional digital sovereignty by allowing governments and businesses to build on verifiable, modifiable infrastructure rather than relying exclusively on proprietary platforms controlled by vendors outside their jurisdiction.

Taken together, these factors demonstrate that open source delivers substantial added value to both the public and private sectors. It reduces cost and lock in, improves security and transparency, accelerates innovation and plays a central role in developing skills and digital capability across the economy.

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?

The EU's open source ecosystem is already a major driver of innovation, competitiveness and digital resilience within the EU. However, its long-term strength depends on strategic measures that address systemic weaknesses, including fragmentation, skills shortages, uneven investment in essential components and limited access to standards and critical infrastructure. To contribute meaningfully to the EU's technological sovereignty and cybersecurity agenda, the next phase of policy intervention must focus on strengthening the foundations of open source, improving coordination across Member States and global partners including the UK, and supporting sustainable, secure and internationally collaborative development. This would require a shift in investment, skills development and contribution to a joined up ecosystem.

Our colleagues in the EU have made specific recommendations which we support. These should be implemented in a way that enhances global collaboration.

4. What technology areas should be prioritised and why?

Open source underpins all digital infrastructure today. The technology areas that should be prioritised are those that consistently appear across industries as high-impact enablers of security, innovation, interoperability and long-term sustainability. This spans hardware and silicon as well as software and there is a need to strengthen production and supply chains in these, through open specifications and open or de facto standards.

Security-critical technologies: Security-focused open source technologies should be a top priority because they underpin the protection and integrity of digital infrastructure across all sectors. Across industries, there is evidence that AI, ML, operation systems, platform environments including cloud and tooling are consistently identified as the technologies most benefiting from open source/ These areas align directly with a priority focus on security-critical languages and components, including memory-safe ecosystems such as Rust, cryptographic libraries, secure build systems, and supply chain and AI tooling. Given the high levels of AI and ML use in safety-critical and regulated sectors, prioritising open, transparent and verifiable AI tooling is essential for detecting vulnerabilities, ensuring

auditability and maintaining public trust. This need is echoed in wider industry studies, which show strong confidence in open source security and a recognised need for investment in secure development and automation tooling.

Interoperability: Open digital ecosystems depend on technologies that enable systems to communicate securely and efficiently. Across several industries, the key benefits of open source include innovation, productivity, transparency and interoperability, particularly pronounced in telecommunications and financial services, where industry standards are vital. Open source supports identity management, secure data exchange, messaging protocols, and open and vendor-neutral standards.

However, the EU still faces interoperability challenges due to a lack of universally adopted open standards, leading to integration friction and higher costs. As such, the EU should prioritise investments in open standards and open alternatives to dominant proprietary platforms.

Public digital infrastructure: Across all sectors, a large proportion of open source contributions are concentrated in areas such as : cloud and containerisation - up to 33% of contributions; CI/CD automation - up to 30%; web and application development - up to 28%; operating systems - between 19% and 37% - sector depending; and IoT and embedded technologies - significant in industrial sectors (21%). These components form the spine of today;s digital services and production systems. Yet, many remain under-maintained because they lack commercial monetisation pathways and rely on volunteer maintainers, creating long-term security and resilience risks.

The EU should prioritise funding to support and maintain public infrastructure through open source software, open standards, open hardware including silicon, open data and AI openness. It is critical that it engages in a collaborative manner with other countries seeking to do the same.

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

An increased use of open source has the potential to deliver significant gains in both competitiveness and cyber resilience across a wide range of sectors. Open source enables shared components, transparent security practices and community driven identification and remediation of vulnerabilities, which together reduce vendor dependence and improve organisational agility. These characteristics are particularly valuable in sectors that operate critical infrastructure or that rely on complex, rapidly evolving digital systems.

The following sectors would benefit immediately from deeper adoption of open source and collaboration around this:

- **Automotive:** Connected vehicle platforms - already rely on collaborative software stacks, and greater openness would drive interoperability, safety and cybersecurity; open charging where standards such as OCPP, could enhance interoperability across the EU and beyond;
- **Mobile:** the sector has shifted to software defined infrastructure and increasingly adopting open source. Transparency and interoperability are essential for trust and network resilience. GSMA, ETSI and other organisations are beginning to understand the value of open source in particular in providing open source implementations for standards.
- **Healthcare:** open technologies improve the transparency and auditability of clinical systems and medical devices, auditability, cybersecurity and trustworthy AI are vital for safe clinical decision making as is interoperability of patient data and systems utilised in that data management;
- **manufacturing and industry:** secure embedded systems and IoT support resilient supply chains and automation; and
- **financial services:** open source underpins secure, scalable transaction systems and reduces reliance on proprietary black box technology. Public administrations can use open source to improve accountability, reduce costs and avoid single supplier dependency, while also accelerating their adoption of secure digital services.

At the same time, several structural weaknesses within the EU open source landscape risk limiting the effectiveness of open source adoption in these sectors. Fragmentation between Member States continues to hinder coordination, resulting in duplicated initiatives and slow progress. Interoperability barriers remain a persistent challenge, including a lack of universally adopted open standards developed within Europe. This increases the cost and complexity of integrating open and proprietary systems and reduces the competitiveness of organisations seeking to modernise their technology stacks.

Skills shortages create another constraint. There is a lack of professionals with lack of expertise in European open source technologies, cloud orchestration and cybersecurity. This shortage limits the ability of organisations to adopt, deploy and maintain secure open source systems. It also slows the rate of digital transformation across sectors that would benefit most from open source approaches. However, the UK has a particularly strong skills base in these areas. Closer EU-UK collaboration would therefore help to address existing shortages within the EU and strengthen overall ecosystem resilience.

Funding sustainability through ecosystem and maintenance, also remains a key barrier to the long-term viability of open source in high impact sectors. Many critical components are maintained by volunteers or small teams with limited resources. The current funding

landscape tends to favour large, established projects and prioritises the development of new features over essential maintenance, security hardening and ongoing support. Without appropriate funding mechanisms, organisations in sectors such as transport, energy, health or financial services may find themselves relying on under-resourced components, which could create cybersecurity and operational risks. Any proposed funding mechanism should be internationally collaborative.

Use of open source and greater collaboration can remove dependency in these and other sectors and allow for diversification and supply chain resilience.

Across all these sectors, the same principles apply. Open source improves cyber resilience by enabling rapid patching, community oversight and forkability in the event of a supply chain compromise. It increases competitiveness by reducing vendor lock in, encouraging innovation and facilitating interoperability. To maximise these benefits, however, barriers relating to fragmentation, standards access, skills, and long-term funding must be addressed. Given the UK's strong skills base and substantial contribution to European open source, ensuring that international collaboration remains central to the EU's approach will further strengthen competitiveness and resilience across these sectors.