Contribution to the European Commission Call for Evidence on “The European Open Digital Ecosystem Strategy”

Submitted by:

Open Knowledge Sweden, Open Knowledge Foundation, Open Knowledge Finland, Open Knowledge Estonia

Date of submission: 2026-02-03

This is a position paper / submission responding to the European Commission's 2026 public consultation / call for evidence on the European Union Strategy “The European Open Digital Ecosystem Strategy” (aimed at setting a strategic approach to the open source sector in the EU that addresses the importance of open source as a crucial contribution to EU technological sovereignty, security and competitiveness and a strategic and operational framework to strengthen the use, development and reuse of open digital assets within the Commission, building on the results achieved under the 2020-2023 Commission Open Source Software Strategy.

Executive Summary

This position paper, submitted by Open Knowledge Sweden, Open Knowledge Foundation, Open Knowledge Finland, and Open Knowledge Estonia, responds to the European Commission's 2026 Call for Evidence on "The European Open Digital Ecosystem Strategy." Drawing on two decades of experience in building and supporting open digital infrastructure, we provide observations and recommendations to advance the EU's strategic approach to open source, emphasizing its role in enhancing technological sovereignty, security, competitiveness, and the Commission's internal use of open digital assets, building on the 2020-2023 Open Source Software Strategy.

The EU open-source sector boasts significant strengths, including one of the world's largest developer communities (nearly 25 million EU-based contributors generating over 155 million annual contributions), alignment with EU principles like transparency and GDPR compliance, and contributions to 70-90% of global software codebases. Successes such as FIWARE, RISC-V, and Simpl demonstrate innovation in AI, cloud, and data spaces, contributing €65-95 billion to EU GDP. However, weaknesses include uneven organizational maturity (only 34%

have formal strategies; 22% have OSPOs), value exploitation by non-EU entities, and barriers like vendor lock-in, underfunding for maintenance, legal concerns, and skill gaps, which hinder adoption, contributions, and scaling.

Open source adds substantial value to public and private sectors by enabling sovereignty, cost savings, reduced lock-in, enhanced security, and innovation. Public examples include France's Nextcloud deployments and Estonia's X-Road for efficient, resilient e-services; private benefits encompass productivity gains (63% of organizations) and competitiveness in telecom and automotive. Key factors: TCO reduction, transparency, and collaborative ecosystems.

To support growth, we recommend dedicated funding (e.g., €1-2 billion via Digital Europe Programme), "open by default" procurement with EU-owned company preferences (EuroStack), sovereign infrastructure (e.g., expanding Codeberg/Gaia-X), public-private partnerships, cybersecurity mandates, and capacity building. Prioritize technology areas like open AI, cloud/edge, cybersecurity tools, RISC-V hardware, and IoT/industrial applications due to high dependencies and sovereignty risks. Amplify OSS in sectors such as public administration, healthcare, automotive, energy, and finance/telecom to boost competitiveness and resilience.

These measures will unlock open source's potential, reducing external dependencies, fostering innovation, and positioning the EU as a global leader in resilient digital ecosystems. We urge swift implementation through pilots and monitoring to achieve quick wins.

Introduction

As pioneers in the social and academic sectors, the Open Knowledge network brings two decades of experience building, stewarding, and supporting open digital ecosystems and open digital infrastructure used by public administrations, civil society, academia, and innovators across Europe and globally. We submit the following observations and recommendations in response to the consultation questions.

Key Questions and Themes

1. Strengths and Weaknesses of the EU Open-Source Sector; Barriers to Adoption, Maintenance, and Contributions

The **EU open-source sector** exhibits notable **strengths** that position it as a vital asset for technological sovereignty, innovation, and alignment with European values. The EU hosts one of the world's largest and most active communities of open-source developers, with nearly 25 million EU-based contributors on developer platforms like GitHub. This is generating over 155 million contributions annually. This ecosystem produces high-quality code that underpins 70-90% of modern software solutions globally, including foundational tools in AI, cloud, and

cybersecurity. European open-source work is particularly well-aligned with EU digital principles, such as transparency, privacy (e.g., GDPR compatibility), interoperability, and ethical considerations, fostering trust and collaboration. Grassroots adoption remains strong, supported by thriving communities, academia-industry partnerships, and contributions to global projects (e.g., scikit-learn, PyTorch, spaCy). Success stories include initiatives like FIWARE, RISC-V investments via the Chips Joint Undertaking, the Simpl programme for secure middleware in data spaces, and emerging efforts in open AI models and hardware. These demonstrate the sector's capacity for innovation, especially in areas like high-performance computing, edge computing, and sovereign alternatives, while contributing significantly to the EU economy (estimated €65-95 billion to GDP in prior studies, with potential for growth).

Despite these strengths, the sector faces significant **weaknesses** that limit its scalability, economic impact, and ability to capture value within Europe. Much of the economic benefit from EU-developed open-source code is exploited outside the EU, often by large non-EU tech companies, due to limited commercialization and market integration of European projects as well as lack of prioritizing EU owned companies in procurements. Organizational maturity is uneven: widespread passive consumption of open source exists, but formal strategies are lacking (only around 34% of organizations have them, per 2025 Linux Foundation Europe research), and Open Source Program Offices (OSPOs) are rare (about 22%). Executive/C-suite recognition of open source's strategic value lags behind employee enthusiasm (86% of employees value it, but only ~60% of leaders do). This results in fragmented efforts, insufficient long-term investment, and challenges in transitioning from research/innovation funding to sustainable scaling and industrial deployment.

The **main barriers** hampering progress fall into two key areas:

(i) Adoption and maintenance of high-quality and secure open source

- High entry barriers and network effects from dominant (often non-EU) proprietary players create vendor lock-in, especially in public procurement and private markets, where tenders often favor or default to proprietary solutions.
- Limited access to growth capital, scalable hosting infrastructures (e.g., EU-based repositories and cloud platforms), and technical support hinders sustainability.
- Maintenance challenges include maintainer burnout, underfunding for long-term upkeep of critical components, and perceived (though often overstated) security risks, despite open source's advantages in transparent vulnerability management.
- Legal/licensing concerns (35%), lack of understanding of non-technical benefits (34%), and compliance fears under regulations like the Cyber Resilience Act slow broader uptake.
- In sectors like SMEs and public administrations, skill gaps, immediate-cost focus over total cost of ownership, and ecosystem fragmentation across Member States exacerbate issues.

(ii) Sustainable contributions to open-source communities

- Legal and intellectual property fears (31% cite licensing concerns, 24% fear IP leakage) discourage private sector involvement.
- Uncertainty about return on investment (ROI) for contributions (28%), combined with limited incentives (e.g., no widespread tax breaks or recognition for code upstreaming).
- Reliance on volunteer or research-driven models without adequate business/sustainability frameworks leads to unsustainable projects.
- Bureaucratic hurdles in public-private partnerships and a cultural gap where open source is valued technically but not always strategically at leadership levels.

Addressing these barriers through targeted EU policy, funding, and infrastructure support could unlock the sector's full potential, reducing external dependencies, enhancing cybersecurity resilience, and boosting EU competitiveness in critical digital technologies.

2. Added Value of Open Source for Public and Private Sectors; Concrete Examples and Factors

Open source delivers substantial added value to both the public and private sectors in the EU, serving as a strategic enabler for technological sovereignty, economic efficiency, democracy, innovation, and resilience. It underpins 70-90% of modern software codebases globally and contributes significantly to the EU economy—estimated at a minimum of €65-95 billion annually to GDP (per European Commission research and related studies), with potential for further growth through increased contributions. By providing transparent, modifiable, and redistributable solutions, open source reduces dependencies on non-EU proprietary vendors, enables and enhances control over the European Union’s and member states’ digital infrastructure, and aligns with core EU principles such as data protection, interoperability, and ethical technology use.

For the public sector, open source offers critical advantages in cost efficiency, security, transparency, and independence from foreign influence. Key factors include:

- **Cost savings and lower total cost of ownership (TCO)**: Avoiding recurring licensing fees frees up budgets for core services. For instance, large-scale deployments in France, such as Nextcloud-based sovereign collaboration platforms, have supported hundreds of thousands to millions of users in public administrations, schools, and regional governments (e.g., Île-de-France's platform for 550,000 students and staff), replacing proprietary alternatives from a non-EU company while ensuring GDPR compliance and data sovereignty.
- **Reduced vendor lock-in and enhanced sovereignty**: Public entities gain flexibility to customize and switch providers. Examples include Germany's Schleswig-Holstein transitioning 30,000 civil servants to LibreOffice and Linux, Denmark's Ministry of Digital Affairs piloting open-source office tools to phase out non-EU based office tools , and France's Gendarmerie migrating 90,000 workstations to Ubuntu-based

GendBuntu—demonstrating long-term independence from non-EU ecosystems and strengthening the EU based IT industry and EU economies.
- **Security and transparency**: Community-driven audits enable faster vulnerability detection and patching, crucial for public trust in critical systems (e.g., Estonia's X-Road for interoperable e-government services).
- **Innovation and public good alignment**: Open source accelerates collaborative development of citizen-centric tools, such as secure data spaces or e-ID systems, while supporting compliance with EU regulations like the Cyber Resilience Act.

For the private sector, open source drives competitiveness through accelerated innovation, productivity gains, and risk mitigation. Recent surveys (e.g., Linux Foundation Europe's 2025 World of Open Source Europe Report) highlight that:

- **Higher productivity and quality**: 63% of European organizations report increased productivity from open source, with 75% noting higher-quality software due to collaborative development and reuse of components.
- **Reduced vendor lock-in and lower costs**: 62% cite avoidance of lock-in and 58% lower software ownership costs as major benefits, enabling faster iteration and resource reallocation.
- **Innovation and market edge**: 69% of respondents believe open source engagement makes organizations more competitive, with 58% seeing it as key to future innovation—particularly in sectors like telecom, automotive, finance, and energy, where companies contribute to shared projects for mutual advantage.
- **Concrete examples**: In telecommunications, providers like Greece's Nova leverage open source (with Canonical support) for cloud infrastructure to control costs and scale efficiently. In automotive and manufacturing, open-source stacks (e.g., via Chips JU investments in RISC-V or software-defined vehicles) enable EU firms to innovate without proprietary dependencies. Open AI models and tools foster rapid prototyping and ethical AI development aligned with EU values.

Overall, the most important factors for assessing added value are **cost (savings and TCO)**, **risk reduction (via transparency and no hidden backdoors)**, **avoidance of lock-in**, **security (community oversight)**, and **innovation speed** (collaborative ecosystems). These benefits often outweigh costs—56% of surveyed organizations report that open source advantages exceed or greatly exceed expenses—while directly supporting EU goals of competitiveness, cybersecurity resilience, and reduced external dependencies. Wider adoption, especially in critical sectors, could amplify these impacts, turning open source into a foundational pillar for Europe's digital future.

3. Concrete Measures and Actions at EU Level to Support Development, Growth, Sovereignty, and Cybersecurity

Concrete measures and actions at EU level should focus on a holistic, multi-year strategy that addresses the full open-source lifecycle—from development and maintenance to sustainability, deployment, market integration, and industrial scaling—while directly advancing

technological sovereignty, competitiveness, and cybersecurity. Building on existing initiatives like the Digital Commons European Digital Infrastructure Consortium (DC EDIC, launched December 2025), the review of the 2020-2023 open-source strategy, the Next Generation Internet programme, FIWARE, Simpl middleware, RISC-V investments, and complementary regulations (e.g., Cyber Resilience Act, NIS2, forthcoming Cloud and AI Development Act), the EU can implement targeted, actionable steps.

Key proposed measures include:

- **Dedicated funding mechanisms beyond R&I grants** to ensure long-term sustainability: Allocate specific budgets under Digital Europe Programme or a new dedicated Open Digital Ecosystems Fund (e.g., €1-2 billion over 2026-2030) for critical open-source projects. This should prioritize maintenance of foundational components (e.g., via bounties or stewardship grants), security audits, and community support to prevent maintainer burnout and vulnerabilities. Expand successful models like Germany's Sovereign Tech Agency to an EU level, funding "digital public goods" in strategic areas.
- **Policy incentives for adoption and contribution**: Introduce an "open by default" principle in public procurement across Member States, mandating evaluation of open-source alternatives in tenders (with weighting for sovereignty, security, and interoperability). Prioritize companies with EU based ownership submitting offers in public procurements when the offering is building on open source and making their solution available open source without vendor lock-in. This is important to increase digital sovereignty and reduce risks for national security or shutdowns of public sectors systems due to foreign influence. Provide tax incentives or fiscal credits for private sector contributions to open-source projects (e.g., upstreaming code or funding maintainers), similar to existing R&D tax schemes. Develop EU-wide certification schemes for secure, sovereign open-source solutions, aligned with the Cyber Resilience Act and NIS2, to build trust and facilitate market entry.
- **Strengthen EU-centred infrastructure and hosting**: Invest in sovereign alternatives to non-EU platforms, such as expanding EU-based code repositories (e.g., Codeberg, or new federated systems such as Forgejo which is enabling Codeberg), cloud platforms (Gaia-X integration), and software-defined infrastructure tools. Support the DC EDIC as a "one-stop shop" for open-source communities, developers, and adopters—providing funding pathways, technical/legal expertise, cross-border collaboration, and reusable building blocks for public administrations.
- **Public-private partnerships and business model innovation**: Foster scalable models through public-private consortia, incubators, and accelerators for open-source startups and SMEs. Promote sustainability frameworks (e.g., dual licensing, foundation-backed models) and partnerships like those in automotive (software-defined vehicle stacks via Chips JU) or AI (open models under GenAI4EU). Encourage large customers (public sector, corporates) to contribute back via mandates or best-practice guidelines.
- **Cybersecurity and sovereignty-focused actions**: Mandate security-by-design in critical open-source projects funded by EU programmes, with regular audits and vulnerability disclosure processes. Prioritize open-source in high-risk sectors (e.g., under

NIS2 supply-chain rules) to reduce third-country dependencies. Develop common criteria for "sovereign" open-source solutions, including transparency, interoperability, and no hidden backdoors.

- **Capacity building and ecosystem growth**: Launch EU-wide training programmes for developers, SMEs, and public administrations on open-source governance, security, and contribution. Support emerging communities via mentorship, hackathons, and visibility platforms to showcase EU high-quality solutions. Monitor progress through dedicated indicators (e.g., adoption rates in public tenders, number of EU-founded projects reaching industrial scale) and periodic external studies.

These measures, combining policy, funding, and infrastructure, would stimulate wider adoption, commoditize expensive proprietary stacks, free resources for innovation, and position open source as a cornerstone of EU's technological sovereignty. They align with Council conclusions on competitiveness (December 2025) emphasizing open standards and reduced lock-in, while complementing ongoing simplifications in digital rules. Implementation could start with pilots in priority areas (AI, cloud, cybersecurity, automotive) to demonstrate quick wins and build momentum toward a resilient, competitive EU open digital ecosystem.

4. Technology Areas to Prioritize and Why

The EU should prioritize the following technology areas in its open digital ecosystems strategy, as they represent critical domains with high external dependencies, rapid innovation potential, and direct relevance to technological sovereignty, competitiveness, cybersecurity, and industrial resilience. These priorities align closely with the Commission's stated focus areas (internet technologies, cloud, AI, cybersecurity, open hardware, and industrial applications such as automotive and manufacturing) and ongoing investments (e.g., RISC-V via Chips Joint Undertaking, Simpl middleware, GenAI4EU, and the forthcoming Cloud and AI Development Act).

1. **Artificial Intelligence (especially open AI models and frameworks)** Why prioritize: The exponential growth of open AI models offers a unique opportunity to reduce reliance on non-EU closed systems (e.g., from US providers), while enabling transparent, ethical, and customizable AI aligned with EU values like privacy and trustworthiness. Open-source AI fosters collaborative innovation, accelerates sector-specific applications (e.g., multilingual models for Europe's diversity), and supports sovereignty by avoiding data-extractive proprietary stacks. Prioritizing this area would boost EU competitiveness in a field where Europe already has strengths (e.g., models from Mistral AI and communities like Hugging Face), while mitigating risks from black-box technologies in high-stakes uses. Investments here could commoditize expensive AI infrastructure and drive industrial uptake under GenAI4EU.
2. **Cloud and Edge Computing** Why prioritize: These form the backbone of digital infrastructure, with ~80% of the EU cloud market dominated by non-EU providers, creating vendor lock-in, data sovereignty risks, and supply chain vulnerabilities. Open-source solutions (e.g., integrated with Gaia-X) enable sovereign alternatives,

interoperability, and cost-effective scaling for SMEs and public sector. Edge computing is essential for low-latency, privacy-preserving applications in IoT and real-time processing. Prioritizing open cloud/edge would reduce dependencies, enhance resilience in critical infrastructure, and complement the Cloud and AI Development Act by providing verifiable, open foundations for hybrid deployments.

3. **Cybersecurity Tools and Software Supply Chain Security** Why prioritize: Open source powers foundational cybersecurity components (e.g., OpenSSL, encryption libraries), but vulnerabilities in widely used projects can have cascading effects. Prioritizing secure open-source tools, governance, and maintenance (e.g., audits, vulnerability management) directly strengthens EU resilience under NIS2 and the Cyber Resilience Act. It addresses supply chain transparency issues, reduces hidden backdoors from proprietary sources, and builds trust in digital infrastructure—critical as cyber threats rise. This area yields high ROI: community-driven patching accelerates response times compared to closed systems.
4. **Open Hardware (particularly RISC-V and related architectures)** Why prioritize: Hardware dependencies (e.g., on non-EU chips) pose strategic risks in computing, edge, and high-performance applications. RISC-V, an open Instruction Set Architecture, enables EU-led innovation in sovereign processors for HPC, edge/IoT, and AI accelerators, as supported by Chips JU projects (e.g., AERO, RISER). Prioritizing open hardware counters geopolitical supply risks, fosters modular designs, and supports emerging ecosystems in edge AI and IoT—key for Europe's industrial competitiveness and reducing reliance on closed architectures.
5. **Internet Technologies, IoT, and Industrial Applications (e.g., Automotive and Manufacturing)** Why prioritize: These interconnected areas underpin critical sectors where open source can disrupt monopolies and enhance resilience. In automotive, open-source software-defined vehicle stacks (via Chips JU) enable faster innovation, supply chain transparency, and independence from proprietary vendors. IoT platforms and internet technologies benefit from open standards for interoperability in smart manufacturing and connected systems. Prioritizing them accelerates standardization, supports EU core industries (e.g., automotive as a flagship), and boosts cyber resilience by allowing verifiable components in high-risk environments.

Rationale for these priorities overall: These areas exhibit the highest combination of dependency risks (non-EU dominance and risk of union security and national security), economic/strategic impact (critical infrastructure and industrial ecosystems), and open-source leverage (transparency, collaboration, rapid iteration). Targeted support would yield outsized benefits: reducing external dependencies, accelerating EU innovation ecosystems, enhancing cybersecurity through community oversight, and enabling market integration of sovereign solutions. Focusing resources here—via funding, partnerships, and policy—would demonstrate quick wins, build momentum for broader adoption, and position open source as a foundational enabler of Europe's long-term technological sovereignty and global competitiveness.

5. Sectors for Increased OSS Use to Boost Competitiveness and Cyber Resilience

Increased use of open source in targeted sectors can significantly boost EU competitiveness by accelerating innovation cycles, reducing costs through shared development, avoiding vendor lock-in, and enabling faster adaptation to market and technological changes. Simultaneously, it enhances cyber resilience by promoting transparent codebases, community-driven vulnerability management, supply chain visibility (e.g., via SBOMs), and verifiable components—aligning with NIS2, the Cyber Resilience Act (CRA), and broader sovereignty goals. Open source disrupts proprietary monopolies, fosters interoperability, and supports resilient digital infrastructure in high-dependency or critical areas.

Key sectors where amplified open-source adoption would deliver outsized benefits include:

- **Public Administration and E-Government** Why: Public sector digital services face high dependencies on non-EU proprietary vendors, leading to lock-in, high costs, and sovereignty risks. Open source enables interoperable, transparent platforms compliant with GDPR and EU digital principles. Increased use would lower TCO, improve cross-border services (e.g., via data spaces and interoperability), and strengthen cyber resilience through auditable code. Examples: Estonia's X-Road (open-source backbone for secure e-services) demonstrates seamless interoperability and resilience; France and Germany's migrations to LibreOffice/Linux in administrations show cost savings and independence. Scaling this EU-wide (e.g., via DC EDIC) would enhance public trust and efficiency.
- **Healthcare** Why: Healthcare relies on secure data sharing, AI diagnostics, and connected devices amid rising cyber threats to patient data and systems. Open source facilitates collaborative development of privacy-preserving tools, ethical AI, and interoperable health data spaces—reducing dependencies on closed vendors and enabling rapid, community-vetted security updates. It boosts competitiveness by lowering barriers for EU startups in medtech/digital health. Examples: Open-source frameworks in EU data spaces for secure health data exchange; potential for reference implementations (as proposed in related roadmaps) using European FOSS building blocks to support personalized medicine and telemedicine while enhancing resilience against ransomware.
- **Automotive and Manufacturing (including Software-Defined Vehicles)** Why: The automotive sector is shifting to software-defined, connected, and electric vehicles, with heavy reliance on proprietary stacks creating supply chain vulnerabilities and innovation bottlenecks. Open-source approaches enable collaborative stacks, modular designs, and faster iteration—critical for EU's industrial core competitiveness. Cyber resilience improves through transparent components and community patching in high-risk connected systems. Examples: Chips Joint Undertaking investments in RISC-V and open software-defined vehicle cores (e.g., SDVoF initiatives, AERO/RISER projects) allow EU OEMs/suppliers to build sovereign alternatives, reduce non-EU dependencies, and integrate open hardware/software for edge/IoT in manufacturing. Wider adoption would accelerate standardization and support green/connected mobility transitions.
- **Energy and Critical Infrastructure (e.g., Smart Grids, Renewables)** Why: Energy systems face growing cyber-physical threats (e.g., attacks on grids) and dependencies on foreign tech for IoT/smart controls. Open source promotes interoperable, verifiable

platforms for smart energy management, enhancing resilience via transparent supply chains and rapid vulnerability fixes. It drives competitiveness in renewables/digitalization by lowering costs and enabling EU-led innovation. Examples: Open-source IoT platforms for energy data spaces; potential extensions of Simpl middleware for secure, sovereign energy applications—reducing risks in critical infrastructure under CER Directive and NIS2.

- **Finance and Telecommunications** Why: These sectors handle sensitive data/transactions with high cyber exposure. Open source supports secure, auditable tools (e.g., blockchain frameworks, encryption libraries) while avoiding lock-in in cloud/telecom infrastructure. It fosters innovation in fintech/regtech and resilient networks. Examples: Open-source contributions in secure transaction platforms; telecom providers using open stacks (e.g., for cloud-native 5G/edge) to enhance sovereignty and patch speed.

Overall rationale: These sectors combine high external dependencies, critical societal/economic impact, and vulnerability to cyber threats—making open source a strategic lever for resilience (transparent auditing, community response) and competitiveness (cost efficiency, collaborative R&D, market agility). Prioritizing them would create spill-over effects: commoditizing proprietary solutions, freeing resources for EU innovation, and demonstrating tangible sovereignty gains through pilots and consortia. This aligns with EU priorities in industrial ecosystems, data spaces, and regulations like CRA/NIS2, turning open source into a multiplier for long-term digital autonomy and prosperity.

EU Trade, aid and emergency assistance need to be aligned as part of the strategy

International aid, development cooperation, and technical assistance should be explicitly integrated as core components of European open digital ecosystems. Open-source technologies and digital public goods offer a democratic, bottom-up model of digital cooperation that prioritises partnership, local ownership, and long-term sustainability over dependence on proprietary vendors.

This approach is particularly relevant in the context of recent and emerging trade and cooperation agreements with partners such as India and Mercosur countries, which are global leaders in open-source development and adoption. Embedding open digital infrastructure into these partnerships enables joint development and shared governance of digital public goods, supports cross-regional collaboration between public administrations, civil society, and developer communities, and allows the EU and its partners to address global challenges such as climate change, public health, migration, inequality, and democratic resilience through interoperable and reusable solutions.

Beyond its internal benefits, this represents a significant diplomatic opportunity. By championing open, interoperable, and publicly governed digital infrastructure, the EU can position itself globally as a trusted partner in digital transformation, a promoter of democratic digital governance, and a leader in sustainable, non-extractive technology cooperation. Investment in

open digital public goods creates shared global assets while reinforcing European values and standards and strengthening the EU's soft power.

Recommendations

- Prioritize EU-based and EEA/EU-owned companies building on open source software and providing their solutions as open source in public procurements. See the industry initiative EuroStack.eu. Make this a priority in the revised EU's public procurement directive.
- Establish a dedicated EU funding programme for the long-term maintenance, security, and governance of critical open digital infrastructure and digital public goods.
- Establish a dedicated EU funding programme to fund research focused on the economic, social and security impact of open technologies powering the open digital ecosystem.
- Promote and create EU-wide platforms for the secure exchange of code, tools and expertise across open source technical teams, to avoid centralisation in commercial infrastructures vulnerable to being affected by a kill switch.
- Create multi-year operational funding instruments for open-source foundations and civic organisations that steward widely used public-interest technologies. Together with it, allocate resources for them to benefit from the emergent public AI infrastructure, including the AI factories.
- Integrate open-source and open-licensing requirements as mandatory into EU-funded digital projects, including digital literacy, public infrastructure, social protection, emergency management and development cooperation as well as all technical assistance programmes. This will enable South - South exchanges, increase the ability to solve problems at scale and optimise the resources.
- Launch joint EU–partner country initiatives with regions such as India and Mercosur, focused on the co-development and shared governance of open technologies, the exchange of local capacities, as well as the distribution of the maintenance and innovation of open digital public goods.
- Align public procurement, funding, and policy instruments to incentivise the adoption of open technologies and contribute back to upstream projects.
- Support shared services, hosting, and support infrastructures to enable public administrations to adopt open-source solutions at scale. This is particularly relevant for municipalities and decentralised entities.
- Strengthen coordination between digital policy, trade, and international partnership instruments to ensure coherence between internal EU objectives and external action.
- Launch initiatives that invite young people to contribute to the development, maintenance, and improvement of this ecosystem.

Conclusion

In conclusion, the Open Knowledge network strongly endorses the European Commission's initiative to advance the European Open Digital Ecosystem Strategy, recognizing open source as an indispensable pillar for achieving technological sovereignty, enhanced cybersecurity, economic competitiveness, and democratic resilience across the EU. By addressing the identified strengths—such as Europe's vibrant developer communities and alignment with core EU values—and overcoming weaknesses like vendor lock-in, underfunding for maintenance, and fragmented adoption, the EU can unlock open source's full potential to reduce external dependencies and foster innovation.

Our recommendations—ranging from dedicated funding mechanisms and "open by default" procurement policies to prioritizing EU-based open source solutions, key technology areas like open AI, cloud/edge, and RISC-V hardware, and amplifying OSS adoption in critical sectors such as public administration, healthcare, and automotive — provide an actionable roadmap for building sustainable, antifragile digital ecosystems. Implementing these measures will not only commoditize proprietary stacks, stimulate SME growth, and generate economic multipliers (e.g., through increased contributions and GDP impacts), but also position Europe as a global leader in ethical, interoperable digital infrastructure.

We urge the Commission to prioritize these proposals in its forthcoming strategy, starting with pilots and monitoring frameworks to ensure measurable progress. The Open Knowledge network stands ready to collaborate with stakeholders to realize this vision, ensuring a resilient digital future for all Europeans. For further discussion, please contact us at contact@okfn.se.

References

GitHub Innovation Graph data on EU developers and contributions. Available from: https://github.blog/news-insights/policy-news-and-insights/help-shape-the-future-of-open-source-in-europe
Published: January 27, 2026.
Nearly 25 million EU-based developers on GitHub, generating over 155 million contributions to public projects in the last year (as of late 2025/Q3 2025 data).

Synopsys. 2024 Open Source Security and Risk Analysis (OSSRA) Report. Available from: https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html
Published: February 2024 (ninth edition).

Open source represents 70-90% of code in modern software solutions globally (consistent with ongoing industry benchmarks referenced in EU documents).

Linux Foundation Europe. The World of Open Source Europe Report 2025: Open Source as Europe's Strategic Advantage. Available from: https://www.linuxfoundation.org/research/world-of-open-source-eu-2025
Published: August 25, 2025 (in collaboration with Canonical).

Key statistics include: 86% of employees value/contribute to open source vs. ~60% of executives recognizing strategic value; only 34% of organizations have formal OSS strategies; 22% have Open Source Program Offices (OSPOs); barriers to adoption (e.g., lack of technical support 40%, licensing/IP concerns 35%, lack of understanding non-technical value 34%); barriers to contributions (e.g., legal/licensing concerns 31%, uncertainty about ROI 28%, fear of IP leakage 24%).

European Commission. Study about the impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy. Conducted by Fraunhofer ISI and OpenForum Europe. Available from: https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and
Published: September 6, 2021 (with ongoing relevance in 2025-2026 policy discussions).

Open source contributes €65-95 billion annually to EU GDP (based on 2018 data, with projections for growth through increased contributions).

European Commission. CALL FOR EVIDENCE: Towards European open digital ecosystems. Ref. Ares(2026)69111 - 06/01/2026. Available from: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16213-European-Open-Digital-Ecosystems_en
Published: January 6, 2026.

References open source as 70-90% of codebases; highlights EU's active developer communities (among the largest worldwide); barriers including high entry barriers, network effects of dominant players, limited access to procurement/capital/infrastructure, value exploitation outside EU, and need for scaling beyond R&I funding.

European Commission. Open Source Software Strategy 2020-2023. Available from: https://commission.europa.eu/system/files/2023-02/en_ec_open_source_strategy_2020-2023.pdf
Approved: October 21, 2020 (under review in 2026 initiative).

Provides context for EU's ongoing efforts, successes (e.g., internal adoption), and recognition of maintenance/sustainability challenges in open-source ecosystems.

Synopsys. 2024 Open Source Security and Risk Analysis (OSSRA) Report. Available from: https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html
Published: February 2024 (ninth edition, with ongoing relevance in 2025-2026).
Open source represents 70-90% of code in modern software solutions globally (77% of all source code/files in audited codebases originated from open source; 96% of codebases contained open source).

European Commission. Study about the impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy. Conducted by Fraunhofer ISI and OpenForum Europe. Available from: https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and
Published: September 6, 2021 (with continued citation in EU policy discussions through 2026).

Open source contributes €65-95 billion annually to EU GDP (based on 2018 data, with projections for growth through increased contributions and adoption).

Linux Foundation Europe. The World of Open Source Europe Report 2025: Open Source as Europe's Strategic Advantage. Available from: https://www.linuxfoundation.org/research/world-of-open-source-eu-2025
Published: August 25, 2025 (in collaboration with Canonical).

Key statistics include: 63% of European organizations report increased productivity from open source; 75% note higher-quality software; 69% believe open source engagement makes organizations more competitive; 58% see it as key to future innovation; 62% cite avoidance of vendor lock-in; 58% lower software ownership costs; 56% report advantages exceeding or greatly exceeding expenses.

Nagle, Frank. Government Technology Policy, Social Value, and National Competitiveness. Harvard Business School Working Paper 19-103. Available from:

https://www.hbs.edu/ris/Publication%20Files/19-103_70f212c8-c4fe-4989-ac99-e03cf8bbf02d.pdf
Published: 2019 (with empirical findings referenced in 2025-2026 EU open-source policy debates).

Enforcement of open-source preferences in French public procurement led to a sustained demand shock, resulting in ~600,000 additional annual open-source contributions, 9–18% annual growth in IT-related startups, and 6.6–14% annual increases in IT employment.

Nextcloud. Île-de-France offers 550,000 students and staff a sovereign cloud collaboration platform. Available from: https://nextcloud.com/blog/ile-de-france-sovereign-cloud-collaboration-platform
Published: December 8, 2025.

Nextcloud-based sovereign collaboration platform deployed by Leviia for Île-de-France regional education system (monlycée.net), supporting over 550,000 students, teachers, and staff across high schools as a GDPR-compliant alternative to proprietary solutions like Microsoft 365.

Schleswig-Holstein state government open-source migration updates. Available from: https://blog.documentfoundation.org/blog/2025/03/13/updates-on-schleswig-holstein-moving-to-libreoffice/ (and related coverage in c't Magazin and EuroStack).
Published: March 13, 2025 (ongoing migration context from 2024-2025 announcements).

Schleswig-Holstein migration of ~30,000 civil servants to LibreOffice and Linux-based systems (e.g., KDE Plasma on distributions like Kubuntu/openSUSE) to achieve data sovereignty, reduce dependencies, and improve long-term cost efficiency.

French Gendarmerie GendBuntu migration. Available from: https://en.wikipedia.org/wiki/GendBuntu (and historical Canonical announcements).
Migration completed phases from 2008-2010s onward.

French Gendarmerie Nationale migrated ~90,000 workstations (across 4,500+ stations) to Ubuntu-based GendBuntu distribution as a secure, sovereign alternative to proprietary systems.

European Commission. CALL FOR EVIDENCE: Towards European open digital ecosystems. Ref. Ares(2026)69111 - 06/01/2026. Available from: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16213-European-Open-Digital-Ecosystems_en
Published: January 6, 2026.
Outlines the review of the 2020-2023 open-source software strategy; emphasizes actions across the OSS lifecycle (development, maintenance, sustainability, market integration); highlights needs for funding beyond R&I, policy incentives (e.g., public procurement preferences), sovereign infrastructure (e.g., EU-hosted repositories/cloud), public-private partnerships, cybersecurity mandates (aligned with NIS2/CRA), and pilots in priority areas like AI, cloud, automotive.

European Commission. Commission to launch Digital Commons EDIC to support sovereign European digital infrastructure and technology. Available from: https://digital-strategy.ec.europa.eu/en/news/commission-launch-digital-commons-edic-support-sovereign-european-digital-infrastructure-and
Published: October 29, 2025 (official establishment; launch December 11, 2025).

Establishes the Digital Commons European Digital Infrastructure Consortium (DC-EDIC) as a collaborative framework for open-source/digital commons; acts as a one-stop shop for communities, developers, public admins; facilitates funding access, technical/legal support, cross-border projects (e.g., European digital workplace), and release under free/open-source licenses; founding members France, Germany, Netherlands, Italy.

European Commission. Digital Europe Programme (DIGITAL). Available from: https://digital-strategy.ec.europa.eu/en/activities/digital-programme
Ongoing programme (2021-2027, with 2026 calls active as of February 2026).

Provides funding for digital technologies including open source, AI, cloud, cybersecurity; supports calls for proposals (e.g., AI Continent, EDIHs, data spaces) that can extend to OSS maintenance, sovereign alternatives, and interoperability; basis for proposed dedicated budgets or new funds (€1-2 billion range suggested in policy discussions).

Sovereign Tech Agency. Sovereign Tech Fund. Available from: https://www.sovereign.tech/programs/fund
Launched 2022 (ongoing as reference model in 2025-2026).

German public investment model funding critical open-source infrastructure (over €24.6 million to 60+ projects by 2025); focuses on maintenance, security audits, sustainability; positioned as scalable EU reference for dedicated stewardship grants/bounties; influences proposals for EU-level expansion or similar mechanisms.

European Commission. Open Source Software Strategy 2020-2023. Available from: https://commission.europa.eu/system/files/2023-02/en_ec_open_source_strategy_2020-2023.pdf
Approved: October 21, 2020 (under review in 2026 initiative).

Internal Commission strategy emphasizing open source adoption, contribution, and sustainability; basis for 2026 review and extension to broader ecosystem support (e.g., policy measures, partnerships).

Gaia-X. Gaia-X: A Federated Secure Data Infrastructure. Available from: https://gaia-x.eu/
Ongoing (federation framework with 2025-2026 advancements).

Promotes sovereign, interoperable cloud/edge via open standards and federation; integration with open-source solutions for data sovereignty; supports EU-centred hosting/infrastructure alternatives to non-EU platforms.

Chips Joint Undertaking (Chips JU). Available from: https://www.chips-ju.europa.eu/
Ongoing (projects active 2023-2026).

Funds open hardware/processor initiatives (e.g., RISC-V in TRISTAN, AERO, RISER projects); supports software-defined vehicle stacks and open-source cores for automotive/industrial applications; enables sovereign alternatives in HPC, edge, IoT.

European Commission. CALL FOR EVIDENCE: Towards European open digital ecosystems. Ref. Ares(2026)69111 - 06/01/2026. Available from: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16213-European-Open-Digital-Ecosystems_en
Published: January 6, 2026.
Defines priority technology areas including internet technologies, cloud, AI (with exponential growth of open AI models), cybersecurity, open hardware, and industrial applications (e.g., automotive/manufacturing, software-defined vehicles); emphasizes high dependency risks, innovation potential, supply chain vulnerabilities, and alignment with sovereignty/competitiveness; references 70-90% OSS in codebases and EU strengths in developer communities/AI.

Synergy Research Group / European Parliament Policy Department. European Software and Cyber Dependencies. Available from: https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/780413/ECTI_ATA(2025)780413_EN.pdf
Published: December 2025.

Cloud infrastructure: AWS, Microsoft Azure, and Google Cloud hold about 70% of the EU market; EU providers' share fallen to roughly 13-15% by 2022-2025; highlights strategic dependencies in cloud underpinning modern software, vendor lock-in, and need for sovereign alternatives.

Gaia-X. Gaia-X: A Federated Secure Data Infrastructure. Available from: https://gaia-x.eu/
Ongoing (with 2025-2026 releases like Danube).

Promotes sovereign, interoperable cloud/edge via open standards, federation, and open-source implementations; supports EU-centred hosting/infrastructure alternatives, trust frameworks, and integration for data sovereignty in cloud/edge computing.

Chips Joint Undertaking (Chips JU). TRISTAN Project. Available from: https://tristan-project.eu/
Ongoing (2023-2026, active in 2025-2026).

Funds expansion and industrialization of European RISC-V ecosystem; creates repository of industrial-quality building blocks for SoC designs in automotive, industrial, HPC, edge/IoT; aims to compete with proprietary alternatives and enable sovereign processors.

Chips Joint Undertaking (Chips JU). Related RISC-V Projects (AERO, RISER, TRISTAN/ISOLDE collaborations). Available from: https://www.chips-ju.europa.eu/ (project references via CORDIS and project sites).
Ongoing (2023-2026).

Supports open hardware initiatives including AERO, RISER for high-performance/edge computing; joint efforts with TRISTAN/ISOLDE for RISC-V CPUs/processors in embedded systems, HPC, edge AI/IoT; counters non-EU chip dependencies.

Mistral AI. Official Site and Model Releases. Available from: https://mistral.ai/
Ongoing (2023-2026 models).

European (French) leader in open-weight/open-source AI models; enables customizable, ethical, transparent AI aligned with EU values; fosters sovereignty by reducing reliance on non-EU closed systems; highlights EU innovation strengths in open AI.

Hugging Face. Open AI Models and Community. Available from: https://huggingface.co/
Ongoing (with EU relevance 2025-2026).

Hosts collaborative open AI models/frameworks (including EU contributions); supports rapid prototyping, multilingual/ethical AI; exemplifies EU ecosystem for open AI innovation and community-driven development.

European Commission. Study about the impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy. Conducted by Fraunhofer ISI and OpenForum Europe. Available from: https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and
Published: September 6, 2021 (with ongoing relevance in 2025-2026 policy discussions).
Estimates open source software contributes €65-95 billion annually to EU GDP (based on 2018 data, with projections for growth through increased adoption and contributions); highlights economic multipliers, reduced dependencies, and benefits in critical sectors like public administration, industrial ecosystems, and data spaces.

Nagle, Frank. Government Technology Policy, Social Value, and National Competitiveness. Harvard Business School Working Paper 19-103. Available from: https://www.hbs.edu/ris/Publication%20Files/19-103_70f212c8-c4fe-4989-ac99-e03cf8bbf02d.pdf
Published: March 3, 2019 (empirical findings referenced in 2025-2026 EU open-source policy debates, including OpenForum Europe analyses).

Enforcement of open-source preferences in French public procurement created a sustained demand shock, leading to ~600,000 additional annual open-source contributions, 9–18% annual growth in IT-related startups, and 6.6–14% annual increases in IT employment; demonstrates positive spill-overs for competitiveness, skills diffusion, and reduced barriers without trade-offs between sovereignty and economic growth.

OpenForum Europe. Open technologies, public procurement and economic impact: lessons from Denmark for Europe's next digital laws. Available from: https://openforumeurope.org/open-technologies-public-procurement-and-economic-impact-lessons-from-denmark-for-europes-next-digital-laws
Published: January 5, 2026.

Discusses Denmark's coordination structures like OS2 and 4S functioning as national Open Source Programme Offices (OSPOs); reduces transaction costs, enables shared repositories/governance/expertise, supports regional ecosystems, reusability, and practical sovereignty; references France's procurement impacts (citing Nagle) and emphasizes OSPOs as "organisational machines" for translating policy into economic/strategic outcomes in public sector.

e-Estonia. X-Road – interoperability services. Available from: https://e-estonia.com/solutions/interoperability-services/x-road
Ongoing (core system since 2001, open-sourced 2016 onward).

X-Road as open-source backbone for secure, interoperable e-government data exchange in Estonia (X-tee); connects public/private sectors, enables cross-border interoperability (e.g., with Finland), supports GDPR compliance, transparency, and resilience; model for sovereign digital infrastructure in public administration.

Chips Joint Undertaking (Chips JU). TRISTAN Project and Related RISC-V Initiatives (including AERO, RISER). Available from: https://www.chips-ju.europa.eu/ (project details via TRISTAN site: https://tristan-project.eu/)
Ongoing (2023-2026, active in 2025-2026).

Funds open hardware/processor ecosystems via RISC-V for automotive (software-defined vehicles/SDVoF), industrial, HPC, edge/IoT; creates industrial-quality building blocks, repositories, and sovereign alternatives to proprietary stacks; empowers EU OEMs/suppliers with modular, transparent components for competitiveness and supply chain resilience.