EUROPEAN ALLIANCE FOR INDUSTRIAL DATA, EDGE AND CLOUD

THEMATIC ROADMAP

THE OPEN SOURCE WAY TO EU DIGITAL SOVEREIGNTY & COMPETITIVENESS

Prepared by the Cloud-Edge Working Group

MAIN CONTRIBUTORS

Stéfane Fermigier (Abilian), Alberto P. Martí (OpenNebula Systems), Jean-Baptiste Piacentino (Clever Cloud), Charles-Henri Schulz (Vates), Arthur van der Wees (Arthur Strategies & Systems)

EDITOR

Dimosthenis Kyriazis (University of Piraeus)

ABOUT THE ALLIANCE & THE OPEN SOURCE TASK FORCE

The European Alliance for Industrial Data, Edge and Cloud [1] brings together businesses, Member States' representatives, and relevant experts to jointly define strategic investment roadmaps to enable the next generation of highly secure, distributed, interoperable, and resource-efficient computing technologies. The work is facilitated by the European Commission's Directorate-General for Communications Networks, Content and Technology (DG CNECT).

The Alliance was established to foster innovation, competitiveness, and growth in Europe's cloud, edge, and IoT sectors, recognizing these technologies as critical building blocks of a sovereign digital future. It brings together the main European Industry players in cloud computing that compiled the *European Industrial Technology Roadmap for the Next-generation Cloud-Edge* in 2023 [2].

Within this framework, a dedicated task force was formed within the Alliance's Cloud-Edge Working Group in order to address the role of Open Source, recognizing it as a key asset in driving European innovation, competitiveness, and independence from excessive control from non-EU technology providers. This document presents the roadmap developed by this task force, outlining a structured approach to enhance Europe's digital autonomy, economic resilience, and environmental sustainability through Open Source technologies developed in, and governed from, the EU.

Following the release of the aforementioned roadmap, specific members of the Cloud-Edge WG have collaborated on developing the current thematic roadmap with a focus on Open Source technologies, challenges, and recommendations. Those members of the WG that have co-authored this roadmap are:

Abilian	OpenNebula Systems
Arthur Strategies & Systems	Vates
Clever Cloud	

The Alliance's Cloud-Edge WG is chaired by Ignacio M. Llorente (OpenNebula Systems), co-chaired by Bjorn Hakansson (TNO) and Arthur van der Wees (Arthur Strategies & Systems), and facilitated by Ana Juan Ferrer (DG CNECT, European Commission). The task force that developed the current thematic roadmap is co-chaired by Alberto P. Martí (OpenNebula Systems) and Jean-Baptiste Piacentino (Clever Cloud).

EUROPEAN ALLIANCE
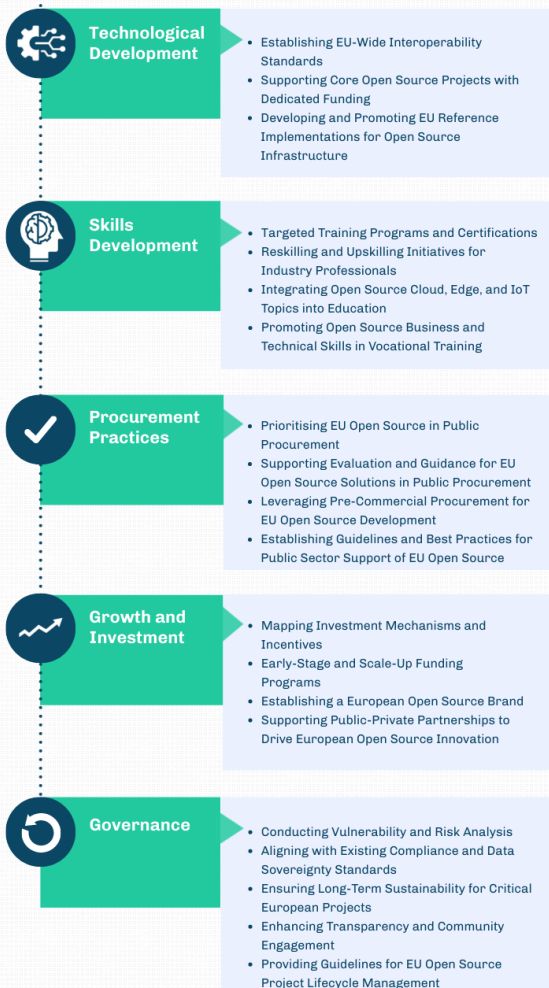FOR INDUSTRIAL DATA,
EDGE AND CLOUD

The Open Source way to EU Digital Sovereignty & Competitiveness

Prioritizing and fostering a robust European Open Source ecosystem

From the Gap

- Interoperability and Standards
- Resource and Funding Sustainability
- Market Awareness and Adoption Barriers
- Skills and Talent Shortage
- Limited Engagement in Collaborative Governance

to 70 key actions across 5 core thematic pillars

Technological Development
- Establishing EU-Wide Interoperability Standards
- Supporting Core Open Source Projects with Dedicated Funding
- Developing and Promoting EU Reference Implementations for Open Source Infrastructure

Skills Development
- Targeted Training Programs and Certifications
- Reskilling and Upskilling Initiatives for Industry Professionals
- Integrating Open Source Cloud, Edge, and IoT Topics into Education
- Promoting Open Source Business and Technical Skills in Vocational Training

Procurement Practices
- Prioritising EU Open Source in Public Procurement
- Supporting Evaluation and Guidance for EU Open Source Solutions in Public Procurement
- Leveraging Pre-Commercial Procurement for EU Open Source Development
- Establishing Guidelines and Best Practices for Public Sector Support of EU Open Source

Growth and Investment
- Mapping Investment Mechanisms and Incentives
- Early-Stage and Scale-Up Funding Programs
- Establishing a European Open Source Brand
- Supporting Public-Private Partnerships to Drive European Open Source Innovation

Governance
- Conducting Vulnerability and Risk Analysis
- Aligning with Existing Compliance and Data Sovereignty Standards
- Ensuring Long-Term Sustainability for Critical European Projects
- Enhancing Transparency and Community Engagement
- Providing Guidelines for EU Open Source Project Lifecycle Management

EXECUTIVE SUMMARY

Over the last decade, as significant geopolitical events and socio-economic trends unfold, Europe is aiming to secure its economic future, uphold its values, and ensure the well-being of its citizens in an increasingly digital world. To this end, genuine digital and technological sovereignty is a prerequisite. This roadmap provides a strategic blueprint for achieving this ambitious goal through the strategic adoption, development, and control of Open Source.

The roadmap recognises that true digital sovereignty extends beyond data control to encompass the underlying technologies that power Europe's digital infrastructure. It identifies the current dominance of non-EU technology providers, particularly in cloud, edge, and IoT, as a significant threat to Europe's strategic autonomy, security, and economic competitiveness. By prioritising and fostering a robust European Open Source ecosystem, this roadmap outlines a path towards a future where Europe controls its digital destiny, free from undue external influence.

The roadmap is driven by four key motivators:

●*Digital and Technological Sovereignty:* Asserting control over Europe's digital infrastructure, reducing reliance on non-EU and/or closed technologies, and ensuring that digital solutions align with European values and interests.
●*Data Security and Compliance:* Safeguarding data privacy and security through transparent, auditable Open Source solutions that comply with European regulations like GDPR and the NIS Directive.

- *Innovation and Economic Resilience:* Fostering a competitive and innovative European digital market by lowering barriers to entry for SMEs, promoting collaborative development, and levelling the playing field.
- *Environmental Sustainability:* Leveraging the adaptability and efficiency of Open Source to reduce the environmental footprint of Europe's digital infrastructure and support the goals of the European Green Deal.

To achieve these goals, the roadmap proposes a series of strategic actions across five key pillars:

- *Technological Development:* Building a resilient technological foundation by developing, adopting, and enforcing open interoperability standards, supporting core European Open Source projects with dedicated funding, and developing sector-specific reference implementations based on European technologies.
- *Skills Development:* Bridging the skills gap by creating targeted training programs, certifications, and educational initiatives focused on European Open Source technologies and standards, fostering a skilled workforce capable of driving innovation and supporting a sovereign digital ecosystem.
- *Procurement Practices:* Reforming public procurement to prioritise Open Source solutions, leveraging public purchasing power to drive adoption, and creating a more accessible and inclusive procurement environment for European SMEs. This includes advocating for "Public Money, Public Code, Open Source First, European Preference" policies.
- *Growth and Investment:* Establishing a sustainable funding ecosystem that supports European Open Source projects through dedicated funding mechanisms, public-private partnerships, and a distinct European Open Source brand or label that promotes excellence and attracts investment.
- *Governance:* Fostering a governance framework that ensures the long-term sustainability, security, and sovereignty of European Open Source projects through proactive risk management, alignment with existing regulations, and a strong emphasis on European leadership and participation in project governance.

The added value of this roadmap is far-reaching, impacting diverse sectors such as public administration, manufacturing, healthcare, and energy. By embracing European Open Source technologies, Europe can enhance security, reduce costs, increase flexibility, drive innovation, and promote sustainability. The recommendations proposed in this roadmap are designed to strengthen Europe's digital sovereignty, boost economic competitiveness, and improve the quality of life for its citizens. To achieve these goals, this roadmap calls on policymakers, industry leaders, the Open Source ecosystem, and all stakeholders to unite behind a shared vision of a digitally sovereign Europe, founded on Open Source principles. By implementing the proposed actions, Europe can unlock the full potential of Open Source, secure its digital future, and establish itself as a global leader in the development and deployment of ethical, responsible, and sovereign digital technologies—*the time for decisive action is now.*

EUROPEAN ALLIANCE
FOR INDUSTRIAL DATA,
EDGE AND CLOUD

TABLE OF CONTENTS

INTRODUCTION

Digitalisation and interconnectedness are reshaping modern society, creating both immense opportunities and significant challenges. To fully harness the benefits of this transformation while safeguarding its values and interests, Europe must build a secure, resilient, and self-sustaining digital infrastructure that serves its citizens, enterprises, and public bodies. This requires a decisive shift towards digital and technological sovereignty, achieved through the strategic adoption and development of European Open Source technologies and solutions.

The roadmap's recommendations are organised into five key pillars: Technological Development, Skills Development, Procurement Practices, Growth and Investment, and Governance. Each pillar addresses specific gaps in the current digital landscape, presenting targeted strategies for building a self-sustaining ecosystem aligned with Europe's regulatory frameworks and values. The roadmap also adopts a phased approach with short-, mid-, and long-term initiatives, offering a realistic path forward that can evolve as Europe's digital needs change. A core principle throughout the roadmap is the prioritisation of European Open Source technologies and solutions, i.e. that are developed under Open Source licenses by, or with significant involvement of, European actors, and in alignment with European values and strategic interests.

This document is structured as follows:

- *1st section — The Need:* Explores the strategic imperatives driving the roadmap, including technological sovereignty, data security and compliance, economic resilience and innovation, and environmental sustainability. It highlights the need for Europe to detach from its dependence on non-EU technologies and build its information systems based on European values and control.
- *2nd section — The Landscape:* Analyses Europe's current cloud, edge, and IoT ecosystem, focusing on existing European Open Source initiatives, research, policy frameworks, and contributions from both public and private entities. It also acknowledges the challenges posed by the dominance of non-EU players in the market.
- *3rd section — The Gap:* Identifies critical challenges hindering Europe's digital objectives, with a focus on interoperability issues stemming from a lack of truly open standards, resource and funding constraints for European projects**,** skills shortages related to European Open Source expertise, market awareness and adoption barriers, and the need for stronger European influence in Open Source governance.
- *4th section — The Proposal:* Outlines the working group's key recommendations across each thematic pillar, offering practical actions to bridge identified gaps and reinforce Europe's digital ecosystem through the strategic development, adoption, and promotion of European Open Source solutions.

- *5th section — The Added Value:* Highlights the transformative impact of European Open Source in cloud, edge, and IoT technologies for various sectors, showcasing the broader societal and economic benefits of this roadmap, including enhanced digital sovereignty, increased competitiveness, improved public services, and more sustainability in the digital sector.

Through supporting a cohesive, sustainable, and sovereign European Open Source ecosystem, the European Alliance for Industrial Data, Edge and Cloud envisions a digital landscape that not only acts as an economic catalyst but also serves as a pillar of Europe's sovereignty and resilience. This roadmap serves as a guide for policymakers, industry leaders, technology developers, and the Open Source community, facilitating collaboration and a shared vision for a secure, transparent, independent, and sustainable digital future in Europe. By fostering unified action and innovative collaboration, and by prioritising Open Source solutions developed and governed in the EU, Europe is positioned to lead in open digital infrastructure, establishing a global standard for responsible, forward-thinking, and sovereign technology governance.

THE NEED FOR A EUROPEAN OPEN SOURCE ECOSYSTEM

Since the late 2010s, and even more so since the COVID crisis and the war in Ukraine, Europe has recognised the imperative of achieving genuine digital and technological sovereignty, decisively reducing its dependence on non-EU technologies, particularly in the domains of cloud computing, edge infrastructure, and the Internet of Things (IoT). These technologies form the backbone of modern digital infrastructure and are essential to both national and economic security. Europe faces mounting pressure to establish a resilient, autonomous, and secure digital ecosystem that meets the needs of its public and private sectors and, crucially, safeguards its fundamental values. This requires not only control over data but also control over the underlying technologies - both hardware & software - that process, store, and manage that data.

The development of a European roadmap for cloud, edge, and IoT technologies, with a strong emphasis on Open Source solutions developed and maintained within Europe, is driven by four critical motivators: digital and technological sovereignty, data security and compliance, innovation and economic resilience, and environmental sustainability. Each of these highlights the necessity of a dedicated strategy that leverages European Open Source technologies to address existing vulnerabilities, close infrastructure gaps, enhance security, and enable European organisations to operate independently, securely, and in full alignment with European values within a trusted digital framework.

Initiatives that focus solely on data sovereignty without addressing the critical need for technological independence risk falling short of achieving these goals. Similarly, initiatives that do not embrace the principles of Open Source and/or the use of genuinely open standards, risk perpetuating vendor lock-in and hindering Europe's ability to control its digital destiny.

Digital and Technological Sovereignty: A Strategic Imperative for Europe

Digital and technological sovereignty have become a strategic priority for Europe, reflecting the urgent need to assert control over its own digital infrastructure, including the entire technology stack from hardware to software, and drastically reduce dependencies on external technology providers. In essential sectors such as healthcare, finance, and public administration, the reliance on foreign-owned cloud, edge technologies, and software platforms for data processing and storage heightens Europe's exposure to significant geopolitical and economic risks. These risks compromise not only data privacy and national security but also operational resilience and the ability to uphold European values in the digital realm. The dominance of non-EU hyperscalers and technology providers in these critical areas poses a direct threat to Europe's ability to control its digital destiny

and necessitates a strategic shift towards solutions that encompass both hardware and software developed and maintained within Europe.

To mitigate these risks, European policymakers and technology leaders are increasingly recognizing the need to advance investments in Open Source infrastructure developed and maintained by European entities. Open Source, with its inherent transparency, security through open auditability, and adaptability, offers a pathway to regaining control. Open Source software allows European organisations to audit, customise, and enhance the code base, offering a level of control and assurance that proprietary software, especially from non-EU sources, often cannot provide. Furthermore, it ensures that the core technologies underpinning Europe's digital infrastructure are developed, maintained, and governed within Europe, aligning with European values, legal frameworks, and strategic interests. By investing in European Open Source (especially in the context of cloud and edge solutions) Europe strengthens its technological autonomy, ensuring that data protection laws are upheld, that critical infrastructure aligns with sovereignty objectives, and that European values are embedded within its digital ecosystem.

Central to achieving digital and technological sovereignty is the strict adherence to open standards. An open standard is a formal specification that is freely accessible, implementable without any restrictions or royalty fees, and compatible with Open Source development and business models. Any standard that discriminates against Open Source, either through licensing, technical, or other restrictions, cannot be considered genuinely open. This principle is essential to avoid vendor lock-in, a common tactic used by non-EU providers to maintain control and limit European autonomy. Initiatives that fail to prioritise the development, adoption, and enforcement of open standards risk perpetuating dependence on foreign technologies. Mandating these open standards, defined and promoted at the European level, can ease the transition from proprietary solutions, create a more cohesive and resilient ecosystem, and, crucially, ensure that Europe retains control over its digital infrastructure.

Furthermore, Europe must move beyond simply adopting open standards to embracing the concept of "enforceable interoperability". This means establishing mechanisms to ensure that these standards are not merely theoretical ideals but are implemented effectively in real-world deployments, guaranteeing genuine interoperability between different systems and providers. Enforceable interoperability, as an approach, shifts the focus from simply adhering to technical specifications to achieving measurable outcomes. It aims at defining clear expectations for interoperability, implementing verification and recourse mechanisms, and fostering an environment where all stakeholders, regardless of their size, can ensure compliance. This includes providing Open Source tools and platforms for testing and validating interoperability, as well as establishing clear processes for addressing non-compliance.

By focusing on practical implementation and enforcement, Europe can avoid the pitfalls of "open washing" and ensure that its Open Source ecosystem contributes towards interoperability and vendor neutrality. The emphasis must be on fostering a complete and resilient European

technology stack, from the hardware to the application layer, to achieve genuine digital sovereignty, actively leveraging the principles of enforceable interoperability to build a truly open and interconnected European digital infrastructure.

Data Security and Compliance: Upholding European Values and Standards

The European Union has set high benchmarks for data security and privacy, most notably through the General Data Protection Regulation (GDPR), which reflects its commitment to safeguarding personal data and upholding fundamental rights. However, reliance on non-EU technology providers introduces potential conflicts and serious security risks, as these providers are often subject to foreign regulations and government interventions, such as the US FISA section 702 [3] and the CLOUD Act [4]. Such extra-territorial legislations grant foreign governments access to data stored or processed by these providers, even if the data belongs to European citizens or is located within the EU. This poses a direct threat to the privacy and security of European data - personal, corporate and governmental alike. Initiatives that do not adequately address these risks will fail to fully protect European data and facilitate foreign surveillance.

Open Source cloud and edge technologies, developed and maintained within Europe, offer a pathway to enhanced data security by allowing European organisations to retain full control over their digital infrastructure within EU jurisdiction. This deployment model, utilizing European Open Source solutions, ensures robust compliance with European regulations by keeping data localised and mitigates risks linked to extraterritorial data access. Furthermore, the ability to independently audit the code of European Open Source software provides an additional layer of security assurance, enabling the detection and remediation of vulnerabilities that might be hidden in proprietary systems.

To achieve robust compliance and enhance security, the roadmap prioritises European Open Source solutions that integrate seamlessly with Europe's existing legal frameworks, including GDPR, the NIS Directive [5], and the ongoing legislative process ePrivacy Regulation. This approach not only strengthens data security but also underscores Europe's commitment to a secure, compliant digital ecosystem governed by transparent, enforceable standards, developed and upheld within Europe. Furthermore, the open nature of Open Source allows for independent security audits, vulnerability assessments, and the development of robust security practices, further bolstering the security posture of Europe's digital infrastructure. By prioritising European Open Source, Europe can ensure that its digital infrastructure is not only compliant with its regulations but also resilient against external threats and aligned with its commitment to data privacy and security.

Innovation and Economic Resilience: A Strategic Asset for Europe

The European cloud, edge, and IoT ecosystem presents a powerful opportunity for economic growth, particularly through the adoption and advancement of European Open Source technologies. Research consistently demonstrates that Open Source software significantly contributes to the economy by reducing software costs, accelerating innovation, and enabling knowledge sharing. Open Source empowers organisations to iterate, adapt, and improve existing solutions, fostering a collaborative approach to innovation that accelerates development cycles and reduces duplication of efforts [6]. This is particularly beneficial for European SMEs, as Open Source provides a lower barrier to entry and allows them to compete more effectively in the global market, especially when these solutions are developed, maintained, and governed within Europe, creating a more level playing field.

Beyond immediate financial savings, European Open Source technologies enhance Europe's economic resilience by encouraging a diversified ecosystem where organisations can collectively address shared challenges, such as interoperability and scalability. Open Source ecosystems allow SMEs to overcome the substantial barriers posed by proprietary, foreign-controlled platforms. By using Open Source tools and standards, developed and governed within Europe, SMEs can compete more effectively, leveraging affordable, customizable infrastructure that helps create a balanced digital market open to companies of all sizes. This fosters a more competitive and diverse European digital market, reducing reliance on a small number of dominant players, many of which are non-EU. The thriving European Open Source ecosystem, supported by initiatives like FOSSEPS and guided by the principles of the Strasbourg Declaration [7], will be a key driver of this economic growth [8].

The Open Source model also encourages European companies to innovate beyond rigid proprietary standards, fostering a collaborative digital landscape that enhances Europe's competitiveness and lessens reliance on costly licensing fees. As such, it positions Open Source as a strategic asset for Europe, driving innovation, creating new jobs and business opportunities, and attracting investments in European tech companies. In turn, this helps create a more resilient economic environment where European companies can better weather market disruptions and continue to deliver on the promise of digital transformation, using technologies aligned with European values. Initiatives that do not prioritise the development, adoption, and governance of European Open Source may inadvertently hinder innovation and economic growth by perpetuating dependence on foreign technologies and limiting the opportunities for European SMEs.

Environmental Sustainability: A Core Principle for European Digital Infrastructure

Sustainability is a central objective within Europe's digital strategy, aligned with broader environmental commitments under initiatives such as the European Green Deal. Data centres and IT infrastructure are substantial energy consumers, and there is growing recognition of the need to reduce the environmental footprint of digital technologies. European Open Source cloud and edge solutions are integral to achieving this goal, offering the adaptability required to minimise energy use, optimise resource efficiency, and extend infrastructure lifecycles. This aligns with the concept of "green computing", which must be a guiding principle in the development and deployment of digital technologies in Europe.

The Open Source model provides organisations with the flexibility to tailor infrastructure to their precise needs, circumventing the constraints of proprietary solutions that often result in resource inefficiency. By enabling continuous updates and optimisations, Open Source software extends hardware lifespans [9], reducing the frequency of hardware replacement and thus minimizing e-waste. This adaptability promotes a sustainable digital infrastructure that aligns with Europe's climate ambitions and supports the development of a circular economy.

As Europe advances toward its environmental objectives, the deployment of European Open Source solutions in cloud and edge infrastructures becomes a critical strategy for reducing energy consumption and fostering responsible IT practices. A roadmap that prioritises environmentally sustainable technology, developed, maintained, and governed within Europe, can empower Europe to build a green, resilient digital ecosystem that supports both economic growth and climate action.

Conclusion: A Unified Vision for a Digitally and Technologically Sovereign Europe

The need for a roadmap dedicated to European Open Source cloud, edge, and IoT technologies is underscored by a convergence of strategic priorities: achieving genuine digital and technological sovereignty, enhancing data security and compliance, driving innovation and economic resilience, and promoting environmental sustainability. These are not just technical goals but fundamental requirements for ensuring Europe's security, prosperity, and adherence to its core values. By focusing on these pillars, Europe can establish a secure, adaptable, and sustainable technology ecosystem that aligns with its long-term ambitions and principles. This necessitates a decisive shift towards prioritising, developing, deploying, and governing Open Source solutions that are conceived, built, maintained, and controlled within Europe. Initiatives that fail to fully embrace this vision, either by neglecting the crucial need for technological sovereignty, by allowing undue

influence from non-EU actors, or by failing to adhere to a strict enough definition of open standards, risk undermining Europe's digital ambitions.

Through collaborative efforts, support for "enforceable interoperability" and unwavering support for European Open Source initiatives, Europe can position itself as a global leader in open, secure, and sovereign digital infrastructure. This roadmap serves as a strategic guide to build resilience and autonomy within Europe's digital landscape, ensuring a future where European organisations operate with security, flexibility, and independence in a rapidly evolving technological world, using technologies that reflect European values and safeguard European interests.

The dominance of non-EU technologies in critical infrastructure is a strategic vulnerability that must be addressed with urgency and determination. The current roadmap, with its strong emphasis on Open Source, open standards, and European control, provides the framework for achieving true digital and technological sovereignty and securing Europe's digital future.

THE LANDSCAPE: EUROPE'S CURRENT OPEN SOURCE CLOUD, EDGE, AND IOT ECOSYSTEM

This section provides an overview of the current landscape in Europe's cloud, edge, and IoT ecosystem, with a particular focus on the role of European-developed and governed Open Source technologies. It examines ongoing research initiatives, commercial activities, and policy frameworks that shape this evolving environment, identifying key trends, strategic initiatives, and emerging challenges within the European context. While Open Source adoption is increasing, the IT market is still largely dominated by non-EU proprietary technologies, particularly from US-based hyperscalers. This highlights the urgent need for a more strategic and concerted effort to foster a truly European Open Source ecosystem. Together, these insights highlight the progress achieved thus far and the areas requiring further action to strengthen Europe's digital and technological sovereignty through Open Source.

Current Research and Policy Initiatives Supporting Open Source Cloud, Edge, and IoT

Europe's commitment to fostering Open Source technologies is evident through targeted research funding and policy priorities, although these efforts need to be significantly amplified and better coordinated. Various initiatives across EU institutions are addressing core challenges in digital infrastructure by promoting security, transparency, and interoperability. However, a stronger emphasis on "made in Europe" Open Source and stricter definitions of open standards are needed to achieve genuine technological sovereignty.

- *IPCEI Cloud:* In December 2023, the European Commission announced its support for an Important project of Common European Interest (IPCEI) on Next-Generation Cloud Infrastructure and Services - the IPCEI-CIS [10]. The Member States leading this project will provide up to €1.2 billion in public funding, which is expected to unlock additional €1.4 billion in private investments. As part of this IPCEI, 19 direct participants, along with more than 100 additional partners, are working together to build a European stack of Open Source technologies for managing and deploying applications across the cloud-edge continuum. This project is supporting the development of the first interoperable and openly accessible data processing ecosystem in Europe. It will develop data processing capabilities, along with software and data sharing tools for enabling federated, energy-efficient, and trustworthy cloud and edge distributed data processing technologies and related AI services. The participating companies will develop Open Source technologies that will allow real-time and low-latency services by distributed computing resources close to the user, thereby reducing the need to transmit large volumes of data to centralised cloud servers. The main challenge will come from

the need to ensure interoperability as part of the IPCEI-CIS Reference Architecture, but also to make sure that additional European cloud providers and tech vendors can easily integrate their products and offerings into this ecosystem—especially those based on European Open Source solutions.

- *Horizon Europe & Digital Europe:* These flagship EU programs are central to research and development funding for next-generation digital technologies.
    - Horizon Europe has allocated significant resources to research in fields such as cloud and edge computing, artificial intelligence, and cybersecurity, fostering collaborations across academia, industry, and government. However, the programme should more explicitly prioritise funding for projects that demonstrably contribute to European technological sovereignty by utilizing and contributing to European Open Source ecosystems.
    - Digital Europe is positioned to drive Europe's digital transformation through investments in AI, HPC, cybersecurity, and digital skills. However, the potential of European Open Source software remains underutilised. Digital Europe needs to dedicate more resources to the development, promotion, and adoption of European Open Source solutions, support SME participation through simplified funding mechanisms and targeted initiatives, integrate Open Source into digital skills programs, and enforce the use of open standards, in all funded projects.
- *Cybersecurity and Data Sovereignty Legislation:* European policies such as the Cyber Resilience Act (CRA) [11], the Digital Services Act (DSA) [12], and the Data Act [13] set high standards for secure, compliant digital solutions, further supporting Open Source adoption. These policies encourage the use of transparent, Open Source technologies with auditable codebases that align with EU data protection requirements. The CRA, in particular, can be leveraged to promote the use of European Open Source in critical infrastructure by mandating security requirements that favour transparent and auditable code. The Data Act complements these efforts by outlining specific data handling, access, and portability requirements essential for cloud and IoT infrastructures, thus accelerating the adoption of secure, sovereign solutions across European markets. However, these regulations need to be accompanied by measures that actively promote the development and adoption of European Open Source alternatives to non-EU proprietary solutions.
- *National and Local Government Support:* Several European countries are advancing Open Source technology adoption through specific public sector policies. For instance, France's *Loi pour une République numérique* [14] and Germany's Online Access Act (OZG) [15] promote Open Source solutions within government procurement, providing a conducive environment for these technologies. The French law (LCEN, 2004) [16], [18] also provides a strong definition of open standards that should be adopted across the EU. However, these national initiatives need to be better coordinated at the European level to avoid fragmentation and ensure a unified approach to digital sovereignty.

These policy frameworks and funding initiatives collectively underscore Europe's commitment to secure, resilient digital infrastructure. However, consistent implementation across EU member states, a stronger emphasis on "made in Europe" Open Source, and stricter enforcement of open standards are essential for fostering a truly integrated and sovereign European Open Source ecosystem.

Commercial and Organisational Contributions to Open Source Technologies

European companies, research institutions, and consortia are actively engaged in the development and deployment of Open Source solutions in cloud, edge, and IoT domains. However, their impact is often overshadowed by the dominance of non-EU technology providers. Noteworthy trends in this domain include:

- *Expansion of European Open Source Cloud and Edge Providers:* Europe has seen a marked increase in cloud providers specializing in Open Source technologies. These providers offer solutions tailored to the regulatory and operational needs of European clients, emphasizing GDPR compliance and data sovereignty. As viable alternatives to foreign proprietary platforms, they play a critical role in enabling organisations to comply with local regulations while maintaining control over their data infrastructure. Such providers are also critical in industries with high compliance requirements, such as finance and healthcare, offering Europe-based cloud solutions that mitigate data jurisdictional risks. However, these European providers often struggle to compete with the scale and resources of non-EU hyperscalers. They need greater support through public procurement, investment, and policy frameworks that favour European solutions.

- *Growth of European Open Source Consortia:* The formation of large, multi-stakeholder consortia in Europe has accelerated the creation of collaborative Open Source projects, but the experiences with certain initiatives reveal critical challenges that must be addressed. These consortia—comprising technology providers, academic institutions, and industry representatives—aim to develop solutions that align with the EU's regulatory and operational priorities, particularly in areas like industrial IoT, edge computing, and data sovereignty.
    - However, projects such as GAIA-X [21] have struggled with high expectations, fragmented governance, and continued reliance on non-EU cloud providers, which has created a gap between their ambitious goals and practical outcomes. GAIA-X, while aiming for data sovereignty, has been criticised for its lack of focus on technological sovereignty, its inclusion of non-EU companies, and its slow progress marked by excessive bureaucracy.
    - Similarly, the FIWARE Foundation [22], which develops and promotes open standards for smart cities and digital infrastructure, has faced slow adoption and limited

engagement beyond certain public sector projects, as well as concerns about its scalability and adaptability to private sector demands.

- o These challenges underscore an urgent need for clearer governance structures that avoid overly complex decision-making, more realistic objectives that balance ambition with practical feasibility, a stronger focus on technological sovereignty alongside data sovereignty, and greater engagement from SMEs to ensure that these projects have both market viability and broader support. Consortia should prioritise the use of European Open Source technologies and adhere to open standards. Without these adjustments, such consortia may fall short of contributing effectively to Europe's digital sovereignty goals and risk becoming dependent on public funding without achieving widespread adoption. Furthermore, they risk being perceived as "Trojan horses" for non-EU interests, undermining the very goals they purport to serve.

- *Collaborations with European Research Institutes:* Many European technology firms partner with research institutes to advance the technical foundations of Open Source cloud and edge computing. Examples include the COGNIT Project [19], where OpenNebula Systems and the Research Institutes of Sweden (RISE) collaborate on developing an AI-enabled serverless framework for edge application management and smart orchestration, or the MetaOS project between Atos and the Universidad Politécnica de Madrid (UPM), which aims to create innovative IoT solutions based on open standards and Open Source software. These collaborations support knowledge transfer and practical innovation, addressing challenges such as low-latency processing, secure data handling, and multi-platform interoperability. Research institutes contribute foundational work in distributed computing, data security, and edge frameworks, strengthening Europe's position in the global Open Source landscape and advancing the adoption of emerging technologies. However, these collaborations need to be scaled up and better coordinated among themselves to maximise their impact. There is also a need to ensure that the results of these collaborations are made available as Open Source, contributed upstream to existing Open Source projects where feasible, in order to contribute to the broader European Open Source ecosystem.

- *Emergence of Specialised IoT Open Source Frameworks:* Open IoT standards (MQTT, CoAP, LwM2M, OPC UA, oneM2M, Zigbee, LoRaWAN...) and European-developed Open Source frameworks such as Eclipse Kura [20] and FIWARE are increasingly adopted across European industries, offering standardised platforms for IoT data processing, device management, and edge-to-cloud integration. These frameworks streamline secure, scalable IoT deployments in sectors such as manufacturing, energy, and agriculture. Building on open standards, they help reduce integration complexity, ensuring that IoT solutions remain adaptable, sustainable, and future-proof. However, many widely adopted IoT frameworks are still dominated by non-EU players. Europe needs therefore to invest more heavily in the development and promotion of its own Open Source IoT frameworks.

Emerging Technologies and Trends in Cloud, Edge, and IoT

The European cloud, edge, and IoT ecosystem is shaped by several technological trends that address critical needs for scalability, data privacy, and operational efficiency. However, many of these trends are currently dominated by non-EU technologies. Europe needs to strategically invest in and promote European Open Source solutions to ensure its technological sovereignty. Key trends include:

- *Edge Computing for Latency Reduction and Data Sovereignty:* Edge computing has become central to Europe's digital infrastructure strategy, especially for latency-sensitive applications. By processing data closer to the source, edge computing minimises latency and reduces the need to transfer large volumes of data to centralised data centers, enhancing data sovereignty. This approach is especially relevant in sectors like manufacturing and smart cities, where real-time data processing is crucial. Projects like CAPE [23] and CLOUDLESS [24] are making significant contributions to this field, but they need more support to compete with non-EU proprietary solutions.

- *Decentralised and Federated Data Models:* Decentralised data models are gaining prominence as a means of addressing privacy and compliance challenges. These models distribute data across multiple nodes rather than relying on centralised storage, enhancing security and resilience. Federated data systems, for example, enable data to remain within specific jurisdictions while still allowing for data sharing and analytics, ensuring compliance with regional regulations while preserving privacy. European research institutions and companies are actively involved in developing Open Source implementations of these models, such as GAIA-X or Pontus-X [25], but more investments are needed.

- *Containerisation and Orchestration for Cloud and Edge Scalability:* Technologies such as Kubernetes and Docker are foundational to cloud and edge scalability. While these technologies are Open Source, their development and governance are largely dominated by non-EU entities. Containerisation allows applications to be deployed consistently across both cloud and edge environments, facilitating rapid scaling and maintaining interoperability across platforms. These technologies are critical for deploying Open Source applications across diverse ecosystems, simplifying operations for organisations that rely on both cloud and edge solutions. Europe needs to invest in developing its own expertise and contributing to the governance of these technologies to ensure they align with European values and interests. Furthermore, Europe should promote the development and adoption of European Open Source containerisation and orchestration solutions.

- *AI and Machine Learning Integration:* AI-powered data processing is transforming cloud, edge, and IoT technologies by enabling advanced analytics, predictive maintenance, and real-time decision-making. Integrating AI and machine learning capabilities into edge devices supports on-device analytics and reduces the dependency on centralised data centres, crucial for applications in industrial IoT and autonomous systems that require immediate insights and low-

latency responses. While many AI/ML frameworks are Open Source, their development is often led by non-EU organisations. Europe needs to foster the development of European Open Source AI/ML frameworks and promote their use in cloud, edge, and IoT applications. Projects like OpenEuroLLM [26] are contributing to this effort. but more investments are needed.

Challenges Facing Open Source Adoption in Cloud, Edge, and IoT

Despite substantial progress, Europe's Open Source landscape still encounters significant challenges that limit broader adoption and impact, particularly in achieving genuine digital and technological sovereignty.

- *Interoperability Barriers:* Although Open Source inherently promotes interoperability, integration challenges remain due to the lack of universally adopted and enforced open standards across cloud, edge, and IoT environments, particularly standards developed and governed by European entities. Organisations using a hybrid mix of Open Source and proprietary tools often encounter compatibility issues. The dominance of proprietary interfaces and APIs from non-EU providers further exacerbates this problem. Developing and mandating EU-wide enforceable interoperability standards is essential to facilitate seamless data exchange and operational consistency.
- *Resource and Funding Constraints:* Many European Open Source projects are resource-constrained, relying on volunteer contributions and sporadic funding. This reliance can result in inconsistent project quality, security vulnerabilities, and challenges in scalability. This is particularly true for projects that are critical to Europe's digital autonomy, as they may lack the resources to compete with well-funded proprietary solutions from non-EU players. The development of long-term funding mechanisms dedicated to European Open Source projects is crucial to ensure continuity, quality assurance, and scalability, safeguarding critical infrastructure from under-resourcing. These funding mechanisms should prioritise projects that demonstrably contribute to European technological sovereignty.
- *Skills and Talent Gaps:* Europe's Open Source ecosystem requires specialised skills in fields such as cloud orchestration, cybersecurity, and IoT systems integration. However, the supply of professionals proficient in these areas, particularly those with expertise in European Open Source technologies, is insufficient to meet demand. Comprehensive training programs and certifications, focused on European Open Source solutions and standards, are essential to bridge this skills gap and cultivate a capable workforce that can enforce and sustain Open Source innovation.
- *Market Awareness and Adoption Hesitancy:* Many European enterprises, particularly SMEs, remain cautious about adopting Open Source cloud and edge solutions, often due to misconceptions about complexity, reliability, and support. The dominance of non-EU marketing narratives often overshadows the capabilities of European Open Source alternatives. Targeted

educational campaigns and pilot programs showcasing successful implementations of European Open Source solutions could demonstrate the value of Open Source solutions and provide practical guidance, fostering trust and reducing perceived barriers to adoption. Public procurement policies that prioritise European Open Source solutions, as outlined in the accompanying position paper, will be crucial in driving market adoption.

Strategic Alliances and Collaborative Projects

Europe's Open Source ecosystem benefits from a network of strategic alliances and collaborative projects that pool expertise and resources across borders. However, these alliances need to be strengthened and more strategically focused on building a truly European Open Source ecosystem.

- *Pan-European Consortia and Networks:* Collaborative networks connect stakeholders across member states to address shared challenges and develop scalable solutions. These consortia typically focus on specific aspects of cloud, edge, or IoT infrastructure, bringing together diverse expertise to tackle technical and regulatory issues. Examples include AIOTI and other initiatives focused on cross-border data transfer protocols and standardised cybersecurity measures for cloud and edge deployments. These consortia need to more explicitly prioritise the use of European Open Source technologies and explicitly adhere to open standards. They should also actively work to counter the influence of non-EU players in the European digital ecosystem.
- *Collaboration with Industry and Policy Bodies:* Organisations such as the Association Professionnelle Européenne du Logiciel Libre (APELL) [27], the OW2 Consortium [28], or the Free Software Foundation Europe (FSFE) [29] play a crucial role in promoting Open Source adoption and shaping policy decisions. By facilitating collaboration among industry stakeholders and policymakers, APELL and similar bodies help align technology development with EU regulations and strategic priorities, ensuring that Open Source evolution supports Europe's objectives for digital sovereignty and security. These organisations should be further empowered and supported to advocate for policies that promote European Open Source solutions and a level playing field for European SMEs.
- *Research Networks and Innovation Hubs:* Europe's innovation hubs and research networks such as HiPEAC serve as platforms for knowledge-sharing, accelerating the transition of academic research into industry applications. These hubs support cross-disciplinary R&D, driving advancements in foundational technologies that benefit multiple sectors, such as distributed computing frameworks and secure data processing. However, these hubs need to focus more explicitly on fostering the development and adoption of European Open Source technologies. They should also work to create stronger links between research, industry, and the Open Source community to ensure that research results are translated into practical solutions and market impact.

Conclusion

Europe's Open Source cloud, edge, and IoT landscape is marked by rapid advancements, collaborative initiatives, and robust policy support. Investments in digital sovereignty, data protection, and environmental sustainability have created an ecosystem that prioritises security, transparency, and interoperability. However, the current landscape is heavily influenced by non-EU technologies and companies. To achieve genuine digital and technological sovereignty, Europe needs to significantly increase its investments and support for European Open Source solutions, to enforce the use of truly open standards, and to foster a more cohesive and strategic approach to Open Source development and adoption. Addressing these challenges will require coordinated efforts across policy, industry, and education.

THE GAP: OBSTACLES TO A SOVEREIGN EUROPEAN OPEN SOURCE ECOSYSTEM

Despite notable advancements in Open Source cloud, edge, and IoT technologies across Europe, several critical gaps persist that prevent the full realisation of a truly sovereign, secure, and resilient digital infrastructure based on European-developed and governed Open Source solutions. These gaps reveal the disconnection between Europe's current technological landscape, still heavily reliant on non-EU technologies, and the strategic objectives it aims to achieve in digital autonomy, interoperability, and innovation. Addressing these gaps is essential for empowering European industries, public institutions, and citizens to harness the full potential of European Open Source digital technologies and to break free from the dominance of non-EU tech giants.

Interoperability and Standards: The Urgent Need for Truly Open, European-Governed Standards

While Open Source technology inherently promotes interoperability, the lack of universally adopted, truly open standards, developed and governed by European entities, across cloud, edge, and IoT platforms within Europe continues to create significant integration challenges. Many organisations operate with a mix of proprietary and Open Source solutions, often leading to a fragmented and inefficient environment where systems fail to align seamlessly. This fragmentation is exacerbated by the influence of non-EU companies that promote their own "open" standards as a façade, while making it hard for competitors to implement such standards, in order to maintain their market dominance.

Without consistent, truly open standards that are free from any restrictions on implementation, especially in Open Source software, integration complexity increases, reducing operational efficiency and adding barriers to the widespread adoption of European Open Source solutions. This requires a shift away from "open washing" and towards a rigorous commitment to genuinely open and enforceable standards, developed and promoted at the European level.

Resource and Funding Sustainability: Securing the Future of European Open Source Projects

A large portion of Europe's Open Source ecosystem, including many projects critical to digital sovereignty, relies on volunteer contributions and sporadic funding. This reliance poses significant risks to long-term stability, as critical projects may lack the resources for ongoing maintenance, security updates, and quality assurance. The current funding landscape often favours large,

established projects, leaving smaller, innovative European initiatives struggling to secure the resources they need to thrive. Funding inconsistencies can lead to project discontinuity or stagnation, weakening the reliability and resilience of Europe's digital infrastructure and making it more vulnerable to external influence.

Without sustainable, dedicated funding mechanisms specifically targeting European Open Source projects that contribute to digital sovereignty, the scalability and continuity of these critical initiatives will remain limited. Europe needs to establish funding models that provide long-term support for these projects, ensuring their viability and fostering a vibrant ecosystem of European Open Source innovation. Ensuring stable and strategic funding is essential to support Europe's strategic priorities, prevent vulnerabilities that may arise from under-resourced projects, and reduce dependence on non-EU funding sources that may come with strings attached.

Market Awareness and Adoption Barriers: Overcoming the Dominance of non-EU Narratives

Despite the economic and operational benefits of Open Source solutions, many European organisations - particularly small and medium-sized enterprises (SMEs) - remain hesitant to adopt them. This hesitancy is often fuelled by misconceptions around complexity, perceived lack of support, and concerns about reliability, often propagated by the dominant market narratives of non-EU technology providers. Many organisations view Open Source solutions as challenging to implement and maintain without dedicated support, especially in sectors that are less familiar with Open Source models. Furthermore, the lack of visibility and promotion of European Open Source alternatives makes it difficult for organisations to even consider them as viable options. For SMEs, adopting Open Source solutions often entails significant organisational and technical changes, which may be perceived as risky without adequate support and guidance.

Targeted educational campaigns, pilot programs, and demonstration projects showcasing the success stories of European Open Source solutions are needed to build trust, reduce perceived risks, counteract the dominant marketing narratives of non-EU vendors, and communicate the value of European Open Source solutions to hesitant stakeholders. Public procurement policies that prioritise European Open Source solutions will also play a crucial role in driving market adoption and creating a more level playing field for European SMEs.

Skills and Talent Shortage: Building a European Workforce for a Sovereign Digital Future

The Open Source cloud, edge, and IoT sectors in Europe face a pronounced skills gap. Although demand is growing for professionals with specialised expertise in these areas, the supply of skilled

workers, particularly those with expertise in Open Source technologies and open standards, has not kept pace. Proficiency in complex areas such as cloud orchestration, IoT systems integration, and cybersecurity is crucial to maintaining secure, efficient Open Source solutions and ensuring they align with European values and regulations.

Yet the shortage of skilled professionals, especially those committed to working on European projects, limits Europe's ability to leverage its Open Source ecosystem fully and slows the pace of innovation. This skills gap also makes Europe more reliant on non-EU expertise, further undermining its digital sovereignty. Addressing this skills shortage through targeted training programs, certifications, and reskilling initiatives that specifically focus on European Open Source technologies and standards is critical to cultivating a workforce capable of advancing Europe's digital autonomy and technological innovation. Furthermore, promoting careers in European Open Source and creating a supportive environment for Open Source professionals within Europe will be essential for attracting and retaining talent.

Limited Engagement in Collaborative Governance: Strengthening European Control and Influence

Europe has made progress in establishing frameworks for collaborative governance in Open Source development, but there remains room for more comprehensive stakeholder engagement across industries and public institutions, particularly in ensuring that governance structures are free from undue influence by non-EU entities. Fragmentation among member states and varying levels of stakeholder participation contribute to a disjointed approach to governance. Furthermore, many Open Source projects, even those with significant European contributions, are governed by foundations or organisations based outside of Europe, potentially leading to decisions that do not align with European interests. Without consistent governance models that prioritise European values and strategic objectives, Europe's Open Source ecosystem lacks the unified oversight and strategic direction needed to sustain long-term innovation and security. A more inclusive and coordinated governance model, with a strong emphasis on European participation and leadership, would provide the guidance, resources, and continuity required to build a secure, cohesive, and truly sovereign Open Source infrastructure that aligns with Europe's strategic priorities for digital sovereignty. This includes supporting the creation and growth of European Open Source foundations and organisations that can provide a counterweight to existing entities largely controlled by Big Tech corporations.

Conclusion

The existing gaps in interoperability, sustainable funding, skills availability, market adoption, and governance present significant obstacles to achieving Europe's vision of a resilient, autonomous

digital infrastructure based on European-developed and governed Open Source cloud, edge, and IoT technologies. The following section will present a series of targeted proposals aimed at closing these gaps, offering actionable recommendations that align with Europe's short-, mid-, and long-term goals, and emphasizing the critical role of Open Source in achieving genuine digital and technological sovereignty for Europe.

THE PROPOSAL

To address the identified gaps and advance Europe's Open Source ecosystem in cloud, edge, and IoT technologies, this section proposes a series of strategic actions. These recommendations are organised according to the roadmap's core thematic pillars: Technological Development, Skills Development, Procurement Practices, Growth and Investment, and Governance. Each recommendation is associated with a temporal dimension—short, mid, or long term—to provide a phased approach that aligns with Europe's long-term goals of digital sovereignty, security, and sustainability.

Pillar 1: Technological Development: Building a Foundation for Digital Sovereignty

Objective: To foster a resilient technological foundation for European-developed and governed Open Source cloud, edge, and IoT solutions by developing and enforcing robust interoperability standards, establishing sustainable funding mechanisms for core European projects, and creating practical reference implementations and fostering their adoption across sectors.

This pillar prioritises the development and adoption of technologies that are not only Open Source but also originate from, and are governed by, European entities, ensuring alignment with European values, regulations, and strategic interests.

Establishing EU-Wide Interoperability Standards: The Cornerstone of a Cohesive Ecosystem (Short-term)

Ensuring enforceable interoperability, based on open standards, is fundamental to building a cohesive, adaptable, and sovereign digital infrastructure across Europe. By developing and enforcing EU-wide open standards tailored to cloud, edge, and IoT environments, the EU can facilitate seamless integration across diverse platforms, reduce dependence on proprietary interfaces, and promote a level playing field for European technology providers. These standards should address compatibility, data portability, and ensure vendor neutrality to reduce dependency on proprietary solutions, particularly those from non-EU providers, and enable cross-border cooperation. Crucially, these standards must be freely accessible, implementable without any restrictions or royalties, and fully compatible with Open Source development and business models.

Key Actions:
- *Define Technical Specifications as Open Standards:* Collaborate with European standards bodies, such as ETSI, CEN-CENELEC, and ECMA, and Open Source organisations (such as APELL, FSFE, OW2, and Eclipse), to create and enforce interoperability standards specific to European Open Source cloud, edge, and IoT environments. These standards must adhere to a definition of open

standards, ensuring they are royalty-free, freely implementable, and compatible with Open Source development and business models. Focus areas should include data representation and transfer protocols (building upon existing open standards like HTTP, MQTT, and CoAP where appropriate), API standardisation (with a focus on RESTful APIs and open specifications like OpenAPI), and compatibility frameworks that ensure seamless integration between European Open Source solutions. The development process must be transparent, inclusive, and driven by European stakeholders.

- *Pilot Interoperability Projects with a European Focus:* Fund pilot initiatives that apply these European-developed standards in real-world contexts, such as cross-border data sharing in healthcare or environmental monitoring. These pilot projects should prioritise the use of European Open Source technologies and involve European SMEs and public administrations. Pilots should evaluate how interoperability standards enhance operational efficiency, reduce integration costs, comply with data sovereignty laws, and promote the adoption of European solutions. They should also serve as testbeds for "enforceable interoperability," providing practical insights into how to ensure that standards are effectively implemented in diverse settings.

- *Mandate Alignment with Regulatory Frameworks:* Mandate that all EU-funded digital infrastructure projects adhere to these interoperability standards. Coordinate standards with existing EU regulations on data protection (GDPR), cybersecurity (NIS Directive, Cyber Resilience Act), and the forthcoming AI Act to simplify compliance and foster regulatory coherence across member states. This alignment should encourage public and private sector adoption by ensuring standards meet Europe's security and privacy requirements and by creating a clear and consistent regulatory environment for European Open Source solutions.

- *Promote and Enforce Open Standards:* Establish mechanisms to promote the adoption and enforce the implementation of these open standards across the EU. This could involve creating a certification program for compliant solutions, providing technical assistance to organisations seeking to adopt the standards, and establishing penalties for non-compliance, particularly for large technology providers that attempt to impose their own proprietary interfaces.

Supporting Core Open Source Projects with Dedicated Funding: Investing in European Digital Sovereignty (Mid-term)

Long-term sustainability of strategic European Open Source projects is essential for a secure, autonomous, and sovereign digital infrastructure. Core projects that support foundational cloud, edge, and IoT capabilities require dedicated funding mechanisms to ensure quality, security, and scalability. These projects should be selected based on their strategic importance to Europe's digital sovereignty, their contribution to the European Open Source ecosystem, and their alignment with European values and regulations. Such projects should receive continuous financial support from European sources to minimize reliance on volunteer contributions or funding from potentially misaligned entities, and promote robust project management practices, long-term roadmaps, and active community engagement.

Key Actions:

- *Establish a Dedicated European Open Source Fund:* Create a dedicated funding program, the "European Open Source Sovereignty Fund" (EOSSF), for essential Open Source projects in cloud, edge, and IoT domains. Focus on projects that enable interoperability based on European-governed open standards, meet European security standards, support compliance with EU data protection laws, and are developed and maintained predominantly by European contributors. Prioritise projects with direct relevance to critical infrastructures, such as healthcare, public administration, energy management, and strategically important emerging technologies. The fund should be substantial enough to provide meaningful support to selected projects and should be managed transparently and accountably, with clear criteria for project selection and funding allocation.

- *Targeted Grants for Security, Maintenance, and Sovereignty Enhancement:* Offer grants for specific activities such as project maintenance, security audits, vulnerability management, performance improvements, and initiatives that enhance the project's alignment with European sovereignty goals. Encourage project teams to implement rigorous quality control practices, adopt secure development lifecycles, and maintain a roadmap that aligns with EU standards and strategic priorities.

- *Partnership with European Research Institutions and OSPOs:* Foster deep collaboration with European academic institutions, Open Source Program Offices (OSPOs), and research centers to involve technical expertise in addressing advanced challenges, such as secure data sharing, edge-device management, and real-time processing capabilities. These partnerships should prioritise the development of European Open Source solutions to these challenges, with a view towards sustainability and applicability. Partnering with universities and research institutions also promotes knowledge transfer, the development of a skilled European workforce, and the development of new technical solutions for Open Source cloud and edge environments, ensuring that research and development efforts are aligned with the needs of the European Open Source ecosystem and contribute to Europe's digital sovereignty goals. Encourage the establishment of OSPOs within these institutions to further promote Open Source adoption and best practices.

- *Develop an Evaluation Guide for European Open Source Solutions:* Provide public procurement officers with practical guides that include criteria for evaluating Open Source solutions in terms of data security, interoperability (based on open standards), alignment with EU data protection standards, and contribution to European digital sovereignty. Include guidance on assessing long-term viability and project sustainability.

Developing and Promoting EU Reference Implementations for Open Source Infrastructure: Showcasing European Excellence (Long-term)

Building trust in European Open Source solutions requires demonstrable, sector-specific implementations that showcase their effectiveness in real-world applications and highlight their advantages over non-EU and/or proprietary alternatives. By developing reference architectures that

are tailored to key sectors, and actively promoting their adoption through public procurement and other incentives, the EU can provide a blueprint for organisations considering Open Source adoption, enabling smoother implementation, showcasing best practices, and fostering a preference for European solutions.

Key Actions:

- *Develop Sector-Specific Reference Architectures Based on European Open Source:* Create Open Source reference implementations that cater to unique sectoral needs in areas like public administration, healthcare, energy, and transportation, utilizing European Open Source technologies as the foundation. For instance, a reference architecture for healthcare might prioritise secure data handling, interoperability with legacy systems, and compliance with GDPR, while utilizing European Open Source solutions for Electronic Health Records (EHRs), data analytics, and telemedicine. These reference architectures should be developed collaboratively, involving experts from the relevant sectors, Open Source developers, and representatives from public administrations.

- *Launch Large-Scale Demonstration Projects with a European Focus:* Collaborate with EU member states on large-scale demonstration projects to illustrate the practical benefits of European Open Source solutions in delivering secure, compliant, and sovereign digital services. These projects should highlight how Open Source frameworks can meet sector-specific compliance requirements, integrate with existing infrastructure, and deliver cost savings and efficiency gains compared to proprietary alternatives. These projects should be highly visible and serve as showcases for the capabilities of European Open Source.

- *Develop and Distribute European Open Source "Playbooks":* Produce comprehensive guidelines, or "playbooks," that outline best practices, operational recommendations, and security considerations for deploying European Open Source solutions in cloud, edge, and IoT environments. These playbooks should serve as practical resources for organisations, helping them to navigate the adoption process, understand the advantages of European solutions, and maximise the benefits of Open Source technology. They should include case studies of successful deployments, templates for implementation plans, and guidance on how to contribute to the development and maintenance of the European Open Source projects being used.

- *Promote Adoption through Public Procurement and Incentives:* Implement policies that actively encourage the adoption of these reference implementations in public procurement. This could involve creating specific procurement guidelines that favour solutions based on the reference architectures, providing financial incentives for their adoption, or establishing a labelling or certification program for compliant implementations.

Summary

Through these strategic actions, Pillar 1 aims to establish a resilient technological foundation for Europe's Open Source ecosystem, addressing immediate needs for interoperability while ensuring

the sustainability of core European projects and providing practical frameworks for sectoral adoption. The subsequent pillars will build on this foundation, addressing skills, procurement practices, investment, and governance to support a cohesive and sustainable ecosystem.

Pillar 2: Skills Development: Building a European Workforce for a Sovereign Digital Future

Objective: To bridge the skills gap in Europe's Open Source cloud, edge, and IoT sectors by establishing targeted training programs, certifications, and educational initiatives that support the development of a skilled European workforce proficient in European Open Source technologies and standards. This pillar focuses on both immediate upskilling needs and long-term integration of Open Source principles and European technological sovereignty within European education systems. The emphasis is on creating a workforce that can not only support but also drive the development and adoption of European Open Source solutions, contributing to Europe's digital autonomy and competitiveness.

Targeted Training Programs and Certifications: Addressing Immediate Skill Gaps (Short-term)

Closing the skills gap is critical for scaling Europe's Open Source ecosystem and ensuring its independence from non-EU expertise. By establishing training programs and certification pathways that validate proficiency in European Open Source cloud, edge, and IoT technologies, the EU can equip a new generation of professionals with the necessary skills to support, expand, and lead this ecosystem.

Key Actions:
- *Industry-Focused Training Workshops with a European Emphasis:* Partner with national governments, digital innovation hubs, European Open Source organisations (such as APELL), and private sector organisations committed to European digital sovereignty to deliver practical workshops, hackathons, and online courses. These programs should address specific skills related to European Open Source tools and platforms, compliance with European regulations (like GDPR, NIS Directive, and the Cyber Resilience Act), and security protocols essential for cloud, edge, and IoT environments. The focus should be on practical, hands-on training that enables participants to immediately apply their new skills in real-world scenarios.
- *Support for SMEs and Public Sector Training with a Focus on European Solutions:* Offer targeted training subsidies or incentives to SMEs and public sector organisations that commit to upskilling employees in European Open Source technologies. This support can help smaller organisations overcome resource constraints that often limit access to specialised training and encourage them to adopt European solutions. Public procurement policies should also favor organisations that demonstrate a commitment to developing Open Source skills within their

workforce. Provide targeted funding and support for training programs focused on European Open Source Cloud/Edge/IoT solutions, addressing the specific skills gap in these areas.

● *Launch Certification Programs for European Open Source Proficiency:* Develop certifications for Open Source proficiency in partnership with European educational institutions, industry bodies, and Open Source organisations. Focus areas should include cloud orchestration (using tools like Kubernetes and OpenStack), cybersecurity, data compliance, interoperability based on European standards, and specific European Open Source platforms and frameworks. Certifications should reflect European standards, build upon European technologies and expertise, and be recognised across member states to support workforce mobility within Europe. These certifications should be positioned as the gold standard for Open Source expertise within the European context.

Reskilling and Upskilling Initiatives for Industry Professionals: Transitioning to a European Open Source Future (Mid-term)

As industries undergo digital transformation, reskilling programs will be essential to help current professionals transition into roles focused on European Open Source cloud, edge, and IoT technologies. Targeted programs should emphasise practical, hands-on skills in high-demand areas, fostering a workforce that can immediately contribute to the European Open Source ecosystem and reduce reliance on non-EU expertise.

Key Actions:
● *EU-Funded Re-skilling Programs with a Focus on European Open Source:* Establish reskilling pathways for professionals in traditional IT and engineering fields, providing a smooth transition into roles in European Open Source development, security, and data management. Programs should focus on skills critical to Europe's digital priorities, such as data sovereignty, interoperability based on European standards, cybersecurity, and proficiency in key European Open Source platforms and frameworks.
● *Collaboration with Industry Partners for Real-World Learning and Placement:* Work with industry leaders committed to European digital sovereignty to create hands-on learning opportunities, such as internships, apprenticeships, and project-based training within European Open Source environments. These programs should prioritise placements within companies and organisations that are actively developing or using European Open Source solutions. Partnerships with tech companies can also foster knowledge sharing, enabling participants to gain experience in applied, industry-relevant skills and build connections within the European Open Source ecosystem.
● *Incentivise Employer Participation and Commitment to European Open Source:* Offer financial incentives to companies that participate in reskilling programs, such as tax credits or subsidies to offset training costs. These incentives should be tied to a commitment from employers to hire and retain professionals who have completed the reskilling programs and to prioritise the use of European Open Source solutions within their operations. Such incentives can encourage

companies to prioritise employee upskilling and create a culture that values continuous learning in Open Source and contributes to the growth of the European Open Source ecosystem.

● *Develop a European Open Source Cloud/Edge/IoT resource platform:* A platform that includes training materials, best practices, case studies, and a directory of European Open Source projects and providers.

Integrating Open Source Cloud, Edge, and IoT Topics into Education: Building a Foundation for Long-Term Growth (Long-term)

Developing a pipeline of skilled professionals for Europe's Open Source ecosystem begins with embedding relevant topics into secondary and tertiary education. By integrating Open Source principles, European technologies, and digital sovereignty concepts into STEM curricula, the EU can cultivate a generation well-prepared to meet the demands of an evolving digital landscape and contribute to a truly sovereign European digital future.

Key Actions:

● *Incorporate European Open Source into STEM Curricula:* Collaborate with educational authorities to ensure that foundational topics in cloud computing, edge computing, IoT, and Open Source principles are integrated into STEM education from secondary school through to university level. The curriculum should emphasise the importance of digital sovereignty and the role of European Open Source in achieving it. Emphasise skills critical for Open Source proficiency, such as programming (using languages like Python, Java, and C++), systems integration, data management, and secure coding practices. Furthermore, the curriculum should highlight specific European Open Source projects, platforms, and frameworks, showcasing their capabilities and encouraging students to contribute to them.

● *Establish European Open Source Centres of Excellence at Universities:* Support the creation of Open Source "centres of excellence" at European universities, promoting research, collaboration, and advanced training in cloud, edge, and IoT technologies with a focus on European Open Source solutions. These centres can serve as incubators for innovation, offering students and researchers the opportunity to work on practical projects, contribute to European Open Source initiatives, and build expertise in Open Source. They should also foster collaboration between academia, industry, and the Open Source community, ensuring that research is aligned with industry needs and contributes to the development of a European Open Source ecosystem.

● *Engage Students through Competitions and Hackathons Focused on European Solutions:* Develop EU-wide initiatives, such as coding competitions, hackathons, and Open Source project challenges, to engage students and encourage them to explore Open Source careers and contribute to European projects. These events should promote practical skills, showcase the capabilities of European Open Source technologies, and offer networking opportunities with

industry professionals working on European solutions, providing students with valuable exposure to real-world applications of Open Source technology within a European context.

Promoting Open Source Business and Technical Skills in Vocational Training: Bridging the Gap Between Education and Industry (Mid- to Long-term)

To ensure that Europe's workforce is equipped with the comprehensive skill set required for European Open Source adoption, vocational training programs should address both technical and business competencies. This dual focus is essential for fostering professionals who not only understand Open Source technology but can also navigate its economic, legal, and organisational implications within a European context.

Key Actions:

- *Introduce European Open Source Business Model Education:* Develop resources and workshops to help students and trainees understand the unique dynamics of Open Source business models, with a focus on successful European examples. Topics should include monetisation strategies, licensing options (including European-specific licenses), go-to-market approaches, and best practices for community engagement, highlighting the importance of contributing to and building upon European Open Source projects.

- *Vocational Training in European Open Source Project Management:* Create vocational training modules that cover project management for Open Source initiatives, including skills in stakeholder management, collaboration within distributed teams, and effective community governance, with a focus on the governance models commonly used in European Open Source projects. These skills are critical for managing Open Source projects that often involve diverse contributors from across Europe and beyond.

- *Certifications for European Open Source Business Proficiency:* Establish a certification for proficiency in Open Source business skills, offering professionals a way to validate expertise in areas like licensing compliance, intellectual property management, and community outreach, with a focus on the European legal and regulatory context. This certification can add value for organisations aiming to establish or scale European Open Source projects effectively and contribute to the growth of a professionalised European Open Source ecosystem.

Summary

Through these targeted programs, Pillar 2 aims to cultivate a workforce capable of driving innovation, implementing secure and compliant European Open Source solutions, and contributing to Europe's digital autonomy. By addressing immediate training needs and fostering long-term educational initiatives, with a strong emphasis on European technologies, standards, and values, Europe can establish a sustainable talent pipeline that meets the demands of its growing Open Source ecosystem and ensures its leadership in a digitally sovereign future. The following pillars will build on this foundation, focusing on procurement practices, investment, and governance to reinforce a cohesive, resilient, and truly European Open Source landscape.

Pillar 3: Procurement Practices: Leveraging Public Purchasing Power for a Sovereign Digital Future

Objective: To enhance the adoption of European Open Source solutions across the public sector by reforming procurement practices, promoting practical evaluation frameworks, and leveraging procurement as a catalyst for digital sovereignty and interoperability.

This pillar emphasises the role of public procurement as a strategic instrument for driving European Open Source innovation, promoting a level playing field for European Open Source providers, and reducing reliance on non-EU proprietary technologies. The focus is on making public procurement a key driver in building a digital infrastructure that is not only based on Open Source but also predominantly built, maintained, and governed within Europe.

Prioritising European Open Source in Public Procurement: Setting the Standard for Digital Sovereignty (Short-term)

Public sector procurement can play a pivotal role in driving demand for European Open Source solutions, directly supporting Europe's goals for transparency, digital sovereignty, and cost efficiency. By prioritising European Open Source in public procurement, the EU can set a precedent for using open, secure, and adaptable technologies in essential services and actively promote the growth of a vibrant European Open Source ecosystem.

Key Actions:
- *Launch a consultation with European public sector bodies and Open Source providers (especially SMEs) to identify and address specific procurement challenges:* This consultation will aim to identify and dismantle existing barriers that hinder public sector organisations from embracing European Open Source solutions, while also gaining a thorough understanding of the diverse needs and challenges faced by different public sector bodies—such as those in healthcare, education, and transportation—in the context of cloud, edge, and IoT technologies. Furthermore, the consultation will gather valuable input on effectively communicating the benefits of European Open Source to public sector decision-makers and explore ways to streamline procurement processes to be more inclusive of smaller, innovative European Open Source providers. Finally, feedback will be solicited on the proposed procurement guidelines to ensure their practicality and effectiveness in achieving the desired outcomes.
- *Adopt "Public Money, Public Code, Open Source First, European Preference" Policies:* Mandate that public sector organisations prioritise European Open Source software in procurement whenever feasible, aligning procurement policies with the EU's digital sovereignty and transparency objectives. This principle extends the "Public Money, Public Code" initiative by adding a crucial "European Preference" clause (often called a "Buy European Act"), ensuring that taxpayer-funded software not only remains accessible and modifiable but also originates from and benefits the European Open Source ecosystem. This will ensure that public funds are used

to strengthen Europe's technological capabilities and reduce its dependence on non-EU providers. Remove barriers related to intellectual property in public procurement related to cloud, edge, and IoT when procuring European Open Source solutions.

- *Develop Procurement Guidelines for European Open Source Solutions:* Develop comprehensive guidelines and resources to support procurement officers in evaluating and selecting European Open Source solutions. These guidelines should cover security standards, data sovereignty requirements, interoperability considerations, and compliance with EU regulations, ensuring that public sector entities can confidently adopt European Open Source technologies. The guidelines should also address the specific challenges faced by SMEs and provide clear criteria for identifying and prioritising European Open Source providers. Mandate the consideration of total cost of ownership (TCO), including exit costs and long-term adaptability. Emphasise the benefits of European Open Source solutions in reducing TCO.

- *Fund Demonstration Projects Showcasing European Open Source:* Launch funded demonstration projects that showcase the successful implementation of European Open Source software in public administration. These projects can serve as reference cases, highlighting the benefits of European Open Source solutions for transparency, cost savings, and scalability in various governmental functions. These projects should specifically demonstrate how European Open Source solutions can replace existing proprietary systems, showcasing their effectiveness and encouraging wider adoption.

- *Define "European Open Source":* Establish clear criteria for what constitutes a "European" Open Source solution. This could include factors such as:
  - *Origin of Development:* A significant portion of the development work should be carried out within Europe.
  - *Governance:* The project's governance structure should be based in Europe or demonstrably aligned with European values and interests.
  - *Community:* A substantial part of the project's community and user base should be located within Europe.
  - *Legal Framework:* The project should be licensed under an OSI-approved license that is compatible with European law and promotes the principles of digital sovereignty.
  - *Data Residency and Processing:* Preference should be given to solutions that store and process data within the EU, complying with GDPR and other relevant regulations.
  - *Contributions:* Organisations maintaining the project should actively contribute to the European Open Source ecosystem.

These criteria will ensure that the "European" label is not misused for "open washing" and that it genuinely reflects a commitment of projects to Europe's digital sovereignty. Alternatively, establish a measure of "European sovereignty" for cloud, edge, and IoT technologies, and use it as a criterion to rank proposals in public procurement.

Supporting Evaluation and Guidance for European Open Source Solutions in Public Procurement: A Practical and Inclusive Approach (Mid-term)

It is essential that public sector organisations make informed procurement decisions that prioritise security, compliance, and quality. However, overly complex or rigid certification programs can create barriers for smaller European Open Source projects and SMEs. A more flexible approach, centred on practical guidance and evaluation resources, would empower public procurement officers to confidently assess European Open Source solutions while minimizing these compliance burdens and fostering a more diverse and competitive ecosystem.

Key Actions:

- *Develop an Evaluation Guide for European Open Source Solutions:* Provide public procurement officers with a practical guide that includes criteria for evaluating Open Source solutions in terms of data security, interoperability, alignment with EU data protection standards, and contribution to European digital sovereignty. This guide should offer a framework that aligns with EU regulations and supports procurement decisions, emphasizing the importance of considering the "European" dimension of Open Source solutions. It should also provide guidance on how to assess the long-term viability and sustainability of Open Source projects, including factors such as community health, governance structure, and development roadmap.

- *Foster Partnerships with European Industry and Standards Bodies for Accessible Evaluation Criteria:* Work with European industry associations, standards organisations, and Open Source foundations to develop evaluation criteria that are both practical and transparent. These partnerships can help ensure that evaluation guidelines meet technical and regulatory needs without requiring costly certification processes. The focus should be on creating criteria that are accessible to SMEs and that promote the adoption of European Open Source solutions.

- *Create a Repository of Recommended European Open Source Solutions:* Develop a publicly accessible repository, building upon existing initiatives like the French Socle Interministériel des Logiciels Libres (SILL) [30], the Italian Catalogo Software [31], or the EuroStack Directory Project (ESDP) [32], listing European Open Source solutions that meet EU evaluation guidelines, enabling procurement officers to identify secure, compliant, and sovereign technologies. This resource can include detailed profiles, highlighting capabilities, compliance considerations, origin of development, governance structure, community involvement, and recommended use cases in public sector contexts. It should also provide information on available support and training resources for each solution.

- *Promote the adoption of technologies developed under the Next Generation Internet (NGI) initiative, or similar initiatives:* Encourage public sector bodies to explore and adopt solutions originally developed through NGI, leveraging the program's focus on Open Source, transparency, and European values. Highlight successful NGI projects (or their successors) in the procurement guidelines and demonstration projects.

This approach offers a balanced pathway, allowing European Open Source projects to demonstrate alignment with EU standards without incurring the costs and complexities of formal certification, thus promoting a more inclusive and practical framework for evaluating Open Source solutions in the public sector and fostering a more competitive and diverse European digital market.

Leveraging Pre-Commercial Procurement (PCP) for European Open Source Development: Fostering Innovation and Tailored Solutions (Long-term)

Pre-Commercial Procurement (PCP) offers a unique opportunity for the public sector to co-develop innovative European Open Source solutions in partnership with European Open Source providers. PCP allows for the creation of tailored solutions that address specific EU needs, particularly in areas where existing technologies (especially those from non-EU providers) may fall short in supporting digital sovereignty, compliance, or interoperability. This approach can be particularly effective in driving the development of European Open Source solutions in strategic areas like cloud, edge, and IoT, where Europe needs to build its own capabilities and reduce its dependence on foreign technologies.

Key Actions:
- *Encourage Cross-Border PCP Initiatives Focused on European Open Source:* Partner with EU member states to initiate cross-border PCP projects that address shared digital infrastructure needs, such as secure data handling, scalable edge computing, or interoperable IoT systems. These projects should specifically target the development of European Open Source solutions that can meet these needs and be deployed across multiple member states. Collaborative PCP projects can drive the development of solutions that are applicable across Europe, fostering economies of scale, consistent compliance with EU standards, and a stronger European Open Source ecosystem.
- *Establish Knowledge-Sharing Platforms for PCP Insights and European Open Source Best Practices:* Create platforms where public sector bodies can share insights, challenges, and best practices from PCP initiatives, with a focus on the lessons learned from developing and deploying European Open Source solutions. This repository of knowledge can serve as a valuable resource for public administrations seeking to adopt Open Source solutions, providing guidance based on successful PCP experiences. It should also highlight the benefits of using PCP to drive innovation in the European Open Source ecosystem.
- *Involve European Open Source Providers in Solution Co-Design:* Actively engage European Open Source providers, particularly SMEs and startups, in the PCP process, fostering collaboration and allowing providers to contribute their expertise in areas like security, interoperability, and cloud management. Co-designing solutions with European Open Source developers ensures that projects address real-world challenges while adhering to EU standards and contributing to the growth of the European Open Source ecosystem. This collaborative approach will help ensure that the solutions developed are not only technically sound but also aligned with the principles of Open Source and the needs of the European public sector.

Establishing Guidelines and Best Practices for Public Sector Support of European Open Source: Ensuring Long-Term Sustainability (Short- to Mid-term)

To ensure effective adoption of European Open Source solutions, the EU should provide clear

guidelines for public sector organisations on managing, maintaining, and supporting Open Source projects, with a focus on ensuring their long-term sustainability and contribution to European digital sovereignty. This includes establishing support frameworks that address common challenges in adoption and integration, especially for organisations that may lack in-house Open Source expertise. These guidelines should also promote the active participation of public sector organisations in the European Open Source ecosystem.

Key Actions:

- *Develop Comprehensive Support Guidelines for European Open Source:* **Publish guidelines that offer public sector organisations practical advice on managing and supporting European Open Source software. These guidelines should include recommended practices for governance, contribution policies, long-term maintenance strategies, and security measures, helping organisations adopt Open Source solutions with confidence. They should also address how organisations can contribute back to the Open Source projects they use, fostering a culture of collaboration and sustainability.**

- *Encourage Public Sector Participation in European Open Source Communities:* **Promote active involvement of public sector representatives in European Open Source communities and development initiatives. Participation enables public sector entities to gain insights into best practices, contribute to project improvements, influence the development roadmap of key projects, and directly influence the development of solutions that meet their specific needs. This will help ensure that European public sector needs are adequately represented in the development of Open Source solutions and that these solutions remain aligned with European values and strategic objectives.**

- *Promote Training for Public Sector Staff on European Open Source:* **Support training programs for public sector IT and procurement teams focused on European Open Source project management, compliance, risk mitigation, and contribution strategies. Training will empower public sector teams to adopt and manage Open Source solutions effectively, helping them maximise the value and longevity of these investments and become active contributors to the European Open Source ecosystem. These training programs should be developed in collaboration with European Open Source organisations and should leverage the expertise of the European Open Source community.**

- *Engage Stakeholders to Refine Procurement Practices:* **Launch a targeted consultation with European public sector bodies and Open Source providers, especially SMEs, to collaboratively identify and address specific procurement challenges. This initiative should aim to pinpoint existing barriers preventing the adoption of European Open Source, understand the unique cloud, edge, and IoT needs of different sectors (e.g., healthcare, education), and gather input on how to effectively communicate the benefits of these solutions to decision-makers. The consultation would also explore ways to simplify procurement for smaller providers and ensure the proposed guidelines are practical and effective in real-world scenarios.**

Summary

By implementing these strategies, Pillar 3 aims to establish procurement practices that actively prioritise and promote European Open Source solutions, streamline compliance processes, and leverage public sector purchasing power as a catalyst for European Open Source innovation and digital sovereignty. These efforts will not only increase the adoption of Open Source technologies across public institutions but also set an example for the private sector, ultimately reducing Europe's reliance on non-EU technologies and driving broader economic benefits by fostering a vibrant and competitive European Open Source ecosystem.

Pillar 4: Growth and Investment: Building a Sustainable Funding Ecosystem for European Open Source

Objective: To establish a sustainable funding ecosystem that prioritises and supports the growth of European Open Source cloud, edge, and IoT technologies across Europe.

This pillar focuses on creating accessible funding mechanisms, fostering private and public investment in European-led projects, and enhancing visibility for European Open Source innovations on a global stage, positioning Europe as a leader in sovereign digital technologies. The emphasis is on building a robust funding environment that not only supports the development of Open Source solutions but also ensures that these solutions are conceived, developed, and governed within Europe, aligning with the principles of digital and technological sovereignty.

Mapping Investment Mechanisms and Incentives: Ensuring Accessibility and Transparency (Short-term)

To support the growth of European Open Source projects, the EU must ensure that funding options are clear, accessible, and tailored to the needs of both early-stage and scaling Open Source initiatives, with a clear preference for technological projects that contribute to European digital sovereignty. By creating a centralised guide to available investment mechanisms, the EU can improve visibility and access to resources, particularly for European SMEs and startups.

Key Actions:
- *Create a European Open Source Investment Platform (EOSIP):* Develop an EU-funded platform, the European Open Source Investment Platform (EOSIP), that consolidates information on available grants, loans, venture capital options, and other funding opportunities specifically for European Open Source projects across various sectors, such as cloud, edge, and IoT. This platform should be easily navigable, updated regularly to reflect new funding opportunities, and prioritise funding sources that align with the principles of digital sovereignty. It should also provide guidance on how to apply for these funds and highlight the benefits of investing in European Open Source.

- *Host Informational Workshops Tailored for European Open Source:* Provide workshops, webinars, and training sessions that introduce European SMEs, startups, and Open Source projects to the funding landscape, detailing application processes, eligibility requirements, and best practices for securing investment. These workshops should emphasise the strategic importance of European Open Source for digital sovereignty and provide guidance on how to align projects with this objective. These workshops can raise awareness about resources available to European Open Source companies and reduce barriers to accessing funds. They should also showcase successful examples of European Open Source projects that have secured funding and achieved significant impact.

- *Establish Partnerships with European Private Investors:* Collaborate with venture capital firms, impact investors, and other private investment bodies that have a demonstrated interest in supporting European technology and digital sovereignty to form a network of EU-focused Open Source venture funds. By encouraging private sector involvement, the EU can attract additional capital into European Open Source ecosystems and support projects that contribute to Europe's digital autonomy. The EU should also explore mechanisms to de-risk private investments in European Open Source, such as providing guarantees or co-investment schemes.

- *Extend the Next Generation Internet (NGI) Initiative with a Focus on Cloud/Edge/IoT:* Sustain funding for the NGI initiative (or a similarly conceived programme based on targeted cascade funding) within the Horizon Europe framework, beyond the 2025-2026 period. Ensure that a significant portion of this funding is dedicated to projects focused on Open Source cloud, edge, and IoT technologies that contribute to European digital sovereignty. Promote synergies with other European funding programs, particularly with those at national level or related to cybersecurity, data infrastructure, and Artificial Intelligence.

- *Regularly evaluate the impact of these funding schemes:* Use metrics that go beyond traditional academic outputs and consider factors like community growth, market adoption, and contribution to European digital sovereignty. The results of these evaluations should inform the long-term direction of these initiatives.

Early-Stage and Scale-Up Funding Programs: Catalysing European Innovation (Mid-term)

To foster innovation and growth within Europe's Open Source sector, it is essential to provide funding solutions that support both early-stage and scaling projects, with a strong preference for those that are European-led and contribute to the continent's digital sovereignty. Dedicated funding programs can address critical development needs, promote economic resilience, and encourage innovative European solutions across cloud, edge, and IoT technologies.

Key Actions:
- *Allocate Dedicated Funding for High-Impact European Open Source Projects:* Identify and fund European Open Source projects with high potential for impact, particularly those that address strategic needs like interoperability, data sovereignty, and cybersecurity. Projects should be

evaluated based on their contribution to European digital sovereignty, their technical excellence, their community support, and their potential for long-term sustainability. By focusing on projects aligned with EU priorities, funding can catalyse innovation and ensure alignment with Europe's digital agenda. The selection process should be transparent and involve experts from the European Open Source community.

- *Establish European Co-Investment Programs:* Develop co-investment models that pair public funding with private sector investment from European sources. These programs can incentivise private investors to support early-stage European Open Source projects while reducing financial risk and promoting joint accountability for project outcomes. These programs should prioritise projects that are strategically important for Europe's digital sovereignty and have the potential to scale across multiple member states.

- *Launch European Open Source Accelerators and Incubators:* Establish accelerators and incubators specifically designed for European Open Source cloud, edge, and IoT technologies. These programs should provide technical support, mentorship, market access resources, and legal guidance on navigating the European regulatory landscape to help startups and SMEs scale their projects effectively and sustainably. These programs should also foster collaboration among European Open Source projects and promote the development of a strong European Open Source ecosystem.

Establishing a European Open Source Brand: Promoting Excellence and Building Trust (Long-term)

A distinct European Open Source brand can enhance the global competitiveness of European innovations, promote EU values of transparency, security, and data sovereignty, and attract international interest in European Open Source technologies. This branding effort will position Europe as a leader in sovereign Open Source, leveraging its investments in sovereignty, sustainability, and open standards. The brand should emphasise the quality, security, and reliability of European Open Source solutions, as well as their alignment with European values and regulations.

Key Actions:

- *Launch a Branding Initiative for European Open Source Projects:* Develop an EU-wide branding strategy that highlights the quality, security, and sovereignty of European Open Source projects. This initiative should focus on elevating the visibility of EU-based projects, communicating the advantages of choosing Open Source solutions developed and governed within Europe, and distinguishing them from non-EU alternatives. The brand should be associated with trust, reliability, and a commitment to European values.

- *Showcase European Open Source Success Stories on International Platforms:* Organise marketing campaigns and participate in global technology conferences to spotlight successful European Open Source projects, emphasizing values like sustainability, digital sovereignty, and data privacy. These campaigns should highlight the unique strengths of European Open Source,

such as its strong community governance, its adherence to open standards, and its commitment to security and privacy. By promoting these case studies, Europe can build a strong reputation as a reliable provider of secure, high-quality Open Source solutions and attract international talent and investment to the European Open Source ecosystem.

● *Form Strategic Partnerships with European Industry Organisations:* Work with European industry bodies and associations to expand the visibility of European Open Source projects within and beyond Europe. These partnerships should focus on promoting the adoption of European Open Source solutions in various sectors and on building a strong network of European companies and organisations committed to Open Source. By strengthening the presence of European solutions in international markets, the EU can attract talent, investments, and collaborations that support the growth of Europe's Open Source ecosystem.

Supporting Public-Private Partnerships to Drive European Open Source Innovation (Mid- to Long-term)

Encouraging collaboration between public and private sectors will be essential to scaling European Open Source solutions, particularly for high-impact projects that require substantial resources. Public-private partnerships can pool expertise, funds, and networks, fostering innovation and ensuring that European Open Source initiatives have the support needed to scale and compete globally.

Key Actions:
● *Establish Public-Private European Open Source R&D Consortia:* Form consortia that bring together public institutions, private companies, (especially SMEs), and research organisations from across Europe to work on high-priority European Open Source projects. These partnerships can address complex challenges in cloud, edge, and IoT that single organisations may lack the resources to tackle independently. They should focus on developing solutions that are strategically important for Europe's digital sovereignty and have the potential to be adopted widely across both the public and private sectors.

● *Incentivise Private Sector Contributions to European Open Source Projects:* Offer tax incentives, grants, or matching funds to private companies that contribute financially or technically to European Open Source initiatives. These incentives can encourage the private sector to participate more actively in Open Source development, enriching the ecosystem and helping projects achieve faster progress. These incentives should be specifically targeted at supporting projects that are deemed critical to Europe's digital sovereignty.

● *Support Knowledge Sharing and Cross-Sector Collaboration within Europe:* Develop platforms and forums for knowledge exchange between public and private sectors, facilitating the sharing of best practices, technical solutions, and project insights related to European Open Source projects. Such platforms can help ensure that both sectors remain aligned on project objectives, quality standards, and regulatory compliance. They can also foster a culture of collaboration and innovation within the European Open Source ecosystem.

Summary

By implementing these strategies, Pillar 4 seeks to create a supportive environment for European Open Source projects to grow and thrive, ensuring a sustainable funding ecosystem that can meet Europe's evolving digital needs. Through targeted investment, strategic branding, and public-private collaboration, this pillar will enable Europe's Open Source ecosystem to remain competitive, secure, sovereign, and aligned with EU priorities.

Pillar 5: Governance: Ensuring the Long-Term Sustainability and Sovereignty of European Open Source

Objective: To establish a cohesive governance framework that ensures the long-term sustainability, security, compliance, and sovereignty of European Open Source cloud, edge, and IoT technologies.

This pillar emphasises proactive risk management, consistent compliance standards aligned with existing regulations, and the establishment of support mechanisms that prioritise European leadership and control within the governance structures of critical Open Source projects. Given the substantial regulatory efforts already underway, particularly the Cyber Resilience Act (CRA), the focus should be on leveraging existing frameworks, providing targeted support to European projects, and fostering a governance model that ensures the European Open Source ecosystem remains resilient, independent, and aligned with European values and strategic interests.

Conducting Vulnerability and Risk Analysis: A Proactive Approach to Security (Short-term)

A proactive approach to risk management is essential for the reliability, security, and sovereignty of Europe's Open Source ecosystem, especially in critical areas like cloud and edge infrastructure. Regular, targeted vulnerability assessments and risk analyses will help address potential threats, ensuring European Open Source projects adhere to Europe's cybersecurity standards and are resilient against external influence or manipulation.

Key Actions:
- *Prioritise Vulnerability Assessments for Critical European Projects***:** Conduct vulnerability assessments for foundational European Open Source projects supporting Europe's digital infrastructure. Emphasis should be on cybersecurity, dependency management (with a focus on reducing reliance on non-EU components), and project sustainability, ensuring that high-impact projects are robust, secure, and under European control.
- *Collaborate with European Cybersecurity Agencies and OSPOs:* Partner with EU cybersecurity agencies, national cybersecurity authorities, and Open Source Program Offices (OSPOs) to develop threat models tailored to European Open Source cloud, edge, and IoT environments. These models should provide actionable insights for project maintainers to enhance resilience

and reduce the risk of vulnerabilities being exploited to undermine European digital sovereignty.

- *Share Findings and Best Practices within the European Ecosystem:* Publish insights and practical guidelines from assessments to the broader European Open Source community, promoting transparency and equipping organisations with effective risk mitigation strategies. This sharing should be facilitated through platforms that prioritise the needs and interests of the European Open Source ecosystem.

Aligning with Existing Compliance and Data Sovereignty Standards: Streamlining Adoption of European Open Source (Mid-term)

Rather than introducing a new compliance framework, the EU should focus on harmonizing European Open Source project requirements with the CRA and other existing standards, ensuring that these projects can easily navigate the regulatory landscape without undue burden. This approach will streamline compliance and avoid redundancies, particularly benefiting European SMEs and smaller projects that would otherwise struggle under additional regulatory weight. Furthermore, it will ensure that compliance efforts contribute to Europe's digital sovereignty goals.

Key Actions:
- *Offer Compliance Guidance Tailored for European Open Source:* Develop interpretive guidance and resources specifically designed to help European Open Source projects navigate CRA, GDPR, and NIS Directive requirements in ways that minimise administrative load and promote their growth and adoption. This guidance should address data protection, sovereignty, cross-border data flow issues, and the specific challenges faced by Open Source projects in demonstrating compliance.
- *Facilitate CRA Certification Accessibility for European Projects:* Support European Open Source projects in understanding and achieving CRA certification as a quality benchmark, providing simplified pathways or checklists for smaller projects. Consider establishing a dedicated support program or fund to assist European projects in obtaining certification.
- *Enable Support for Documentation and Auditing with a Focus on European Resources:* Provide resources (such as templates, guidelines, and potentially funding) to assist project maintainers, particularly in European projects, in developing the documentation needed to meet CRA and related compliance standards, fostering an Open Source ecosystem that meets regulatory requirements without imposing additional frameworks. Promote the use of European auditing and security assessment services to ensure that these processes are aligned with European standards and values.

Ensuring Long-Term Sustainability for Critical European Projects: A Strategic Imperative (Long-term)

The long-term sustainability of foundational European Open Source projects is essential for Europe's digital resilience and sovereignty. EU initiatives should aim to provide ongoing support

and oversight while promoting knowledge transfer, talent development, and European leadership within these projects, building a sustainable foundation without enforcing rigid governance structures. The focus should be on ensuring that these critical projects remain under European control and are not susceptible to external pressures or takeovers that could compromise their alignment with European interests.

Key Actions:

- *Secure Long-Term Funding for Core European Open Source Infrastructure:* Allocate stable funding to support essential European Open Source projects aligned with EU priorities, such as digital sovereignty, security, and interoperability. Funding should target maintenance, security, community engagement efforts, and initiatives that strengthen European leadership within the project's governance structure. This funding should be substantial and long-term, providing these projects with the stability they need to thrive and contribute to Europe's digital infrastructure.

- *Establish Mentorship Programs Focused on European Talent:* Invest in mentorship and training programs that develop the next generation of maintainers for critical European projects. These programs should focus on transferring skills and technical expertise within Europe, ensuring that these projects remain under European stewardship in the long term. They should also promote best practices in Open Source governance, security, and community management, tailored to the European context.

- *Form a European Open Source Advisory Board:* Establish an advisory body comprising representatives from public institutions, industry experts, European Open Source organisations, and the European Open Source community to oversee the funding and guidance of critical projects. This body would serve as a resource for best practices and governance support, promote the adoption of European Open Source solutions, and advocate for policies that strengthen Europe's digital sovereignty. It should also play a role in identifying and mitigating potential risks to the long-term sustainability of European Open Source projects. Establish formal and informal channels for regular dialogue and consultation with the European Open Source community when developing policies related to cloud, edge, IoT, and digital sovereignty. Establish a high-level coordinator or task force for Open Source technologies within the European Commission and in the European Political Strategy Centre (EPSC).

Enhancing Transparency and Community Engagement: Fostering a European Open Source Ethos (Short- to Mid-term)

Transparency and community engagement are key to building trust and promoting active participation in governance. The EU's approach should focus on promoting open and inclusive governance in funded projects, with a particular emphasis on fostering a strong European presence and influence within these communities, fostering alignment with Europe's values of openness, collaboration, and sovereignty.

Key Actions:

- *Promote Transparent Governance in EU-supported European Projects:* Require EU-funded European Open Source projects to follow transparent decision-making and accountability practices. Governance policies should encourage public documentation of contributions, decision-making processes, and funding allocations. They should also promote the use of open and accessible communication channels, ensuring that all stakeholders, particularly those within Europe, can participate in the project's governance.

- *Support European Community Involvement in Governance:* Actively encourage and facilitate the participation of European community members in governance activities, such as consultations, public forums, and contributor voting. These efforts will promote inclusivity, responsiveness to stakeholder needs, and ensure that European voices are heard within the governance structures of these projects. This could involve providing funding for community events, translation services, and other initiatives that lower the barriers to participation for European developers and users.

- *Facilitate Community Input in European Policy Development:* Create channels for European Open Source communities to contribute to EU policy discussions affecting their ecosystem, fostering alignment between policy frameworks and the practical needs of developers and users. This will ensure that policies are informed by the expertise and experience of the European Open Source community and that they support the growth and sustainability of European Open Source projects.

Providing Guidelines for European Open Source Project Lifecycle Management: Supporting Sustainable Development (Mid-term)

Project lifecycle management is vital to the quality, security, and long-term viability of Open Source projects. Instead of mandating a new framework, the EU should focus on disseminating best practices for project management, specifically tailored to the needs and context of European Open Source projects, helping maintainers navigate the complexities of development, maintenance, and eventual end-of-life transitions.

Key Actions:

- *Publish Best Practice Guidelines for European Project Lifecycles:* Develop and distribute EU-backed guidelines for European Open Source project lifecycles, covering stages from development to end-of-life. Guidelines should emphasise security, documentation, community engagement, and sustainability, drawing on best practices from successful European Open Source projects. They should also address the specific challenges faced by European projects, such as navigating the EU regulatory landscape and securing long-term funding.

- *Offer Resources for Maintenance and End-of-Life Support for European Projects:* Provide resources to assist European projects in managing long-term maintenance and planning for responsible end-of-life transitions, ensuring security and minimizing disruptions for users. This could involve creating a dedicated support program or fund to help projects wind down in a

sustainable manner, ensuring that their codebases remain available and that users are given adequate time and support to migrate to alternative solutions.

- *Encourage Comprehensive Documentation and Knowledge Sharing within the European Ecosystem:* Encourage European projects to document key aspects of their technology and governance, facilitating knowledge transfer and continuity across contributors and maintainers. Promote the use of open and accessible documentation platforms and encourage the translation of documentation into multiple European languages.

Summary

By implementing these strategies, *Pillar 5* aims to establish a governance approach that promotes security, compliance, sustainability, and, crucially, European leadership and control within the Open Source ecosystem. Instead of creating additional compliance frameworks, it emphasises support and alignment with existing EU regulations, fostering a balanced ecosystem that maintains critical infrastructure, enhances community engagement, and supports Europe's long-term goals for digital sovereignty and technological independence.

THE ADDED VALUE

Implementing the proposed roadmap for European Open Source cloud, edge, and IoT technologies holds transformative potential across a multitude of sectors, contributing significantly to Europe's objectives of economic resilience, digital sovereignty, and environmental sustainability. This roadmap is a strategic foundation for long-term progress, offering immediate and lasting benefits to various industries and public services, driving innovation, enhancing competitiveness, and improving the lives of European citizens. Through a robust and well-supported European Open Source ecosystem, Europe can unlock efficiencies, reinforce security, foster a culture of innovation based on European values, and strengthen its global standing as a leader in digital technologies.

Sector-Specific Benefits

The transformative potential of this roadmap extends across numerous sectors. Here we highlight some key examples:

Public Administration: A Foundation for Digital Sovereignty

Adopting European Open Source cloud and edge solutions in public administration is foundational for advancing Europe's digital sovereignty. With European Open Source technologies, public institutions can maintain greater control over data handling, storage, and processing while ensuring compliance with Europe's regulatory and security frameworks. This control is paramount for safeguarding sensitive citizen data and ensuring that public services are delivered in accordance with European values and legal requirements. This alignment enhances transparency, fosters accountability, and strengthens public trust in government services.

Added-Value Highlights:
- *Enhanced Security and Compliance:* European Open Source technologies offer full transparency, allowing public institutions to rigorously monitor and control data management practices. This visibility aligns with GDPR and other EU data protection laws, providing a level of compliance that enhances citizen trust and ensures that data is handled according to the highest European standards.
- *Reduced Dependency on non-EU Providers:* By adopting European Open Source infrastructures, European governments can significantly reduce reliance on foreign technology providers, decreasing vulnerabilities related to external influence, data breaches, and potential surveillance. This enhances the resilience of public services and safeguards Europe's digital sovereignty.
- *Cost-Effective Digital Transformation:* European Open Source solutions lower procurement and licensing costs, enabling public administrations to adopt cutting-edge technologies within budget constraints, ultimately benefiting taxpayers while accelerating digital transformation

initiatives. This also frees up resources that can be reinvested in further developing and improving public services.

- *Increased Transparency and Accountability:* Open Source allows for greater scrutiny of government systems, promoting transparency and accountability in public administration.

Manufacturing and Industry 4.0: Driving Innovation and Competitiveness

In manufacturing, European Open Source IoT and edge solutions are vital for realizing Europe's Industry 4.0 vision, where smart factories leverage real-time data and automation to enhance production efficiency, reduce waste, and adapt to shifting market demands. European Open Source technologies provide the flexibility needed for scalable, future-proof solutions that support the transformation of EU industrial sector and enable European manufacturers to compete globally.

Added-Value Highlights:

- *Predictive Maintenance and Real-Time Monitoring:* European Open Source IoT frameworks provide manufacturers with access to solutions for monitoring equipment conditions in real-time, anticipating maintenance needs, and reducing operational costs, resulting in minimised downtime and maximised productivity.
- *Improved Interoperability and Flexibility:* European Open Source standards enable seamless integration of new technologies into existing systems, allowing manufacturers to avoid vendor lock-in and keep their operations adaptable to evolving needs and industry advancements.
- *Sustainable Production Practices:* By optimizing resource use, European Open Source edge and IoT solutions contribute to reducing energy consumption and waste, aligning manufacturing practices with the EU's Green Deal and advancing toward a circular economy.
- *Enhanced Innovation and Customisation:* The open and collaborative nature of European Open Source allows manufacturers to customise solutions to their specific needs and to contribute to the development of new functionalities, fostering a culture of innovation within the European manufacturing sector.

Healthcare and Medical Innovation: Transforming Patient Care and Advancing Research

European Open Source technologies in healthcare enable secure and efficient management of sensitive patient data, supporting critical applications such as telemedicine, diagnostics, and interoperability across healthcare systems. These solutions empower healthcare providers to deliver responsive, patient-centred care while upholding stringent data protection standards, thereby enhancing both patient trust and operational efficiency. Furthermore, they provide a platform for European researchers and medical professionals to collaborate and innovate, driving advancements in medical science and improving patient outcomes.

Added-Value Highlights:

- *Data Security and Patient Privacy:* European Open Source frameworks provide fully auditable codebases, allowing healthcare providers to manage sensitive data securely and ensure

compliance with data protection regulations, a necessity in the healthcare sector. This is particularly important in the context of GDPR and other European regulations that prioritise patient privacy.

- *Enhanced Telemedicine and Remote Monitoring:* Leveraging trusted European Open Source IoT and edge solutions, healthcare providers can deliver remote care and diagnostic services, monitor patient health in real-time, and respond proactively to changes in patient conditions, reducing strain on physical healthcare facilities and improving access to care, especially in remote or underserved areas.

- *Interoperability Across Systems:* European Open Source protocols facilitate seamless data exchange across healthcare systems, enabling coordinated care, improving patient outcomes, and accelerating advancements in medical research through shared insights and standardised processes. This interoperability is crucial for building a connected and efficient European healthcare system.

- *Accelerated Medical Research:* European Open Source platforms enable researchers to share data, collaborate on projects, and develop new treatments and therapies more efficiently, leading to faster medical breakthroughs and improvements in public health.

Energy and Environmental Sustainability: Powering a Greener Future

In the energy sector, European Open Source cloud, edge and IoT solutions support efficient energy management and align with the EU's climate targets, such as those under the European Green Deal. By contributing to optimizing energy consumption, integrating renewable resources, and reducing the environmental impact of data centres, European Open Source technologies play a pivotal role in Europe's sustainable energy transition.

Added-Value Highlights:
- *Optimised Energy Management:* Real-time monitoring and control of energy grids through European Open Source solutions enhance grid reliability and reduce waste by enabling data-driven decisions and automated adjustments.

- *Support for Renewable Energy Integration:* European Open Source IoT and edge frameworks allow for the effective integration of renewable energy sources into the grid, balancing supply and demand and facilitating a shift toward cleaner, distributed energy generation.

- *Reduced Data Centre Energy Consumption:* With resource-efficient, customizable European Open Source cloud solutions, Europe can reduce data centre energy usage, thereby contributing to a sustainable digital infrastructure and supporting climate initiatives like the Green Deal.

- *Enhanced Energy Efficiency:* European Open Source solutions enable the development of smart energy management systems that optimise energy consumption in buildings, cities, and industries, contributing to significant energy savings and emissions reductions.

Other Sectors: The benefits of this roadmap extend to many other sectors, including but not limited to Transportation, Agriculture, Finance, Education, Smart Cities, Space Industry. openEO is an example in this last sector [33]. openEO is a federated, cloud-based, open source environment that enables users to process and analyse large volumes of Earth Observation (EO) data from satellites. The specific examples and applications will vary depending on the sector, but the underlying principles of enhanced security, reduced costs, increased flexibility, and greater control through European Open Source solutions remain consistent.

Long-Term Strategic Benefits: Securing Europe's Digital Future

The roadmap's recommendations extend beyond immediate sectoral benefits, offering long-term strategic value that reinforces Europe's goals of digital sovereignty, economic competitiveness, and environmental responsibility.

- *Strengthened Digital and Technological Sovereignty:* By fostering a self-sufficient European Open Source ecosystem, Europe can secure control over critical digital infrastructures, drastically reduce dependency on non-EU technologies, and safeguard sensitive data from extraterritorial influence. This approach supports Europe's autonomy in managing and 0protecting its digital assets and ensures that its digital future is shaped by European values and interests.
- *Economic Competitiveness and Innovation:* European Open Source technologies enable collaborative development and knowledge sharing, stimulating innovation and fostering a competitive marketplace. By supporting European Open Source initiatives, Europe can drive advancements across sectors, empowering SMEs and startups to compete alongside larger entities and strengthening Europe's position as a leader in digital technology. This will create new economic opportunities, generate high-skilled jobs, and enhance Europe's overall economic resilience.
- *Environmental Responsibility:* European Open Source solutions promote sustainable practices by supporting energy efficiency, extending hardware lifespans, and fostering responsible technology use. This alignment with the EU's climate and environmental objectives reinforces Europe's commitment to sustainable development, ensuring that digital growth goes hand-in-hand with environmental stewardship.
- *A More Resilient and Adaptable Digital Infrastructure:* A strong European Open Source ecosystem provides Europe with the flexibility and agility to adapt to future technological changes and emerging challenges. By having control over the core technologies that underpin its digital infrastructure, Europe can ensure its long-term resilience and its ability to respond effectively to unforeseen events or disruptions.

Conclusion: A Call to Action for a Sovereign Digital Europe

This thematic roadmap by the European Alliance for Industrial Data, Edge and Cloud represents a strategic blueprint for establishing a resilient, secure, and open digital ecosystem that aligns with Europe's long-term goals for digital sovereignty, economic resilience, and environmental sustainability. This roadmap, by focusing on European Open Source technologies, not only addresses current needs but also lays the groundwork for a future where Europe leads in innovation, data sovereignty, and sustainable development.

In addressing interoperability through genuinely open standards, resource sustainability through strategic funding for European projects, talent development focused on building a skilled European workforce, and market engagement, the roadmap offers actionable steps across five essential pillars: Technological Development, Skills Development, Procurement Practices, Growth and Investment, and Governance. Each pillar encompasses short-, mid-, and long-term initiatives designed to bridge gaps in the current landscape, ensuring that European cloud, edge, and IoT technologies operate seamlessly and securely, free from dependency on external providers, and under European control. This roadmap not only empowers Europe's industries and public institutions but also strengthens its competitive standing in a global digital economy increasingly shaped by Open Source innovation.

Through dedicated support for truly open interoperability standards, foundational European Open Source projects, and a comprehensive governance framework, the roadmap fosters an ecosystem that is adaptable, self-sustaining, and collaborative. By engaging stakeholders across government, industry, and academia, the Alliance promotes a unified, pan-European approach to developing and deploying cutting-edge digital technologies. Public procurement policies that prioritise European Open Source, structured training programs focused on building European expertise, and incentivised investment mechanisms targeting European innovation further reinforce this ecosystem, promoting widespread adoption, skill development, and ongoing innovation.

The added value of this roadmap extends far beyond technological advancement. European Open Source cloud, edge, and IoT solutions unlock benefits for sectors that are vital to Europe's future, driving progress and improving the lives of citizens across the continent. This roadmap emphasises not only security and compliance but also environmental responsibility and economic inclusivity. Together, these elements contribute to Europe's broader mission of creating a digital ecosystem that reflects its values of transparency, sustainability, and trust.

As Europe moves forward with this vision, the roadmap will serve as a guiding framework for addressing emerging challenges and harnessing opportunities in the digital landscape. By committing to these goals, the European Alliance for Industrial Data, Edge and Cloud proclaims its commitment to a future where Europe leads in digital innovation and autonomy, setting global standards for an open, resilient, and sustainable digital infrastructure.

REFERENCES

[1]   Cloud Alliance, https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance

[2]   European Industrial Technology Roadmap for the Next-generation Cloud-Edge,
        https://ec.europa.eu/newsroom/dae/redirection/document/102590

[3]   FISA section 702: https://www.intel.gov/foreign-intelligence-surveillance-act/fisa-section-702

[4]   CLOUD Act: https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf

[5]   NIS: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

[6]   Impact of open source software and hardware on technological independence, competitiveness and
        innovation in the EU economy, https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-
        source-software-and-hardware-technological-independence-competitiveness-and

[7]   Strasbourg declaration, https://www.transformation.gouv.fr/espace-presse/strasbourg-declaration-
        common-values-and-challenges-european-public-administrations

[8]   The Open Source Market in France & Europe: https://cnll.fr/news/2022-survey-the-open-source-market-
        in-france-europe/

[9]   ADEME report: Sustainability and Sovereignty Through Open Source, https://euro-
        stack.com/blog/2025/1/ademe-sustainability-report

[10]   IPCEI-CIS, https://8ra.com

[11]   Cyber Resilience Act (CRA), https://eur-lex.europa.eu/eli/reg/2024/2847/oj

[12]   Digital Services Act (DSA), https://eur-lex.europa.eu/eli/reg/2022/2065/oj

[13]   Data Act, https://eur-lex.europa.eu/eli/reg/2023/2854/oj

[14]   Loi pour une Républiqe numérique, https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000033203039

[15]   Germany's Online Access Act (OZG), https://www.recht.bund.de/bgbl/1/2024/245/VO.html

[16]   LCEN: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164

[17]   German Open Source Observatory, https://interoperable-europe.ec.europa.eu/collection/open-source-
        observatory-osor/news/germanys-ozg-20-favors-open-source-solutions

[18]   LCEN 2004, https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000006421544

[19]   COGNIT Project, https://cognit.sovereignedge.eu/

[20]   Eclipse Kura, https://eclipse.dev/kura/

[21]   GAIA-X, https://gaia-x.eu/

[22]   FIWARE, https://www.fiware.org/

[23]   CAPE, https://cordis.europa.eu/project/id/101189899/de

[24]   CLOUDLESS, https://cloudlab-urv.github.io/cloudless.github.io/

[25]   Pontus-X, https://blockchain-observatory.ec.europa.eu/european-blockchain-sandbox-announces-
        selected-projects-first-cohort_en

[26]   OpenEuroLLM, https://openeurollm.eu/

[27]   Association Professionelle Européenne du Logiciel Libre (APELL), https://apell.info/

[28]   OW2: https://www.ow2.org/

[29]   Free Software Foundation Europe (FSFE), https://fsfe.org/index.en.html

[30]   French Socle Interministériel des Logiciels Libres (SILL), https://code.gouv.fr/sill/

[31]   Italian Catalogo Software, https://developers.italia.it/it/search

[32]   EuroStack Directory Project (ESDP), https://euro-stack.com/

[33]   openEO, https://dataspace.copernicus.eu/analyse/openeo

ANNEX I: ADDITIONAL BIBLIOGRAPHY & REFERENCES

This bibliography provides the foundational evidence and intellectual underpinnings for the strategic imperatives, data, and recommendations outlined in this roadmap, which focuses on achieving digital sovereignty in the critical domains of Cloud, Edge, and IoT through the strategic adoption of Open Source.

Some of these documents diagnose the critical challenges facing Europe's Cloud, Edge, and IoT ecosystems: the significant economic cost of technological dependency on a few non-EU hyperscalers; the acute legal and security risks posed by extraterritorial legislation; and the geopolitical implications of a market where foundational infrastructure is controlled from abroad.

In response, some of these documents articulate a clear and actionable path forward. The bibliography covers the central role of Open Source as a strategic lever to regain control. It details concrete policy proposals for procurement and investment aimed at building a robust European Cloud-to-Edge continuum, and highlights the practical initiatives required to foster a resilient, competitive, and truly sovereign European digital ecosystem.

I. Ecosystem Survey & Economic Justification

These documents establish the high-level political and strategic context, providing the core economic data and vision for why Open Source is a critical asset for Europe.

Study about the impact of Open Source software and hardware on technological independence, competitiveness and innovation in the EU economy (Blind et al., European Commission, 2021)

Source: https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and

Relevance: The foundational EU study providing the core economic data (€65-€95 billion GDP contribution) and a cost-benefit ratio for Open Source investment, which is a central argument of the report.

The Impact of Open Source on the EU Economy (Wladawsky-Berger, I., & OpenForum Europe, 2022)

Source: https://openforumeurope.org/wp-content/uploads/2022/05/The-Impact-of-Open-Source-on-the-EU-Economy.pdf

Relevance: An accessible summary and analysis of the above cornerstone EC study, making its key findings widely understandable.

The Value of Open Source Software (Manuel Hoffmann, Frank Nagle, Yanuo Zhou, HBS Working Paper, 2024)

Source: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4693148

Relevance: This recent Harvard Business School paper provides a powerful, updated economic valuation of Open Source, estimating its global demand-side value in the trillions of dollars and reinforcing its immense economic importance.

Technological dependence on American software and cloud services: an assessment of the economic consequences in Europe (CIGREF, 2025)

Source: https://www.cigref.fr/technological-dependence-on-american-software-and-cloud-services-an-assessment-of-the-economic-consequences-in-europe

Relevance: A critical report from a leading French association of large enterprises, quantifying the economic risks of technological dependency and advocating for a strategic resilience.

2022 survey: The open source market in France & Europe (CNLL, Numeum, & Systematic Paris-Region, 2022)

Source: https://cnll.fr/news/2022-survey-the-open-source-market-in-france-europe/

Relevance: Provides specific market size, growth projections, and employment data for Europe's Open Source sector, quantifying the growth in key areas like cloud, AI, and IoT.

World of Open Source: Europe Spotlight 2023 (Linux Foundation Research & LF Europe, 2023)

Source: https://www.linuxfoundation.org/research/2022-europe-spotlight

Relevance: Offers a comprehensive overview of the state of Open Source in Europe, its key projects, and strategic importance from a leading global foundation.

2024 IoT & Embedded Developer Survey Report (Eclipse Foundation, 2024)

Source: https://outreach.eclipse.foundation/iot-embedded-developer-survey-2024

Relevance: As a major European-based foundation, this survey offers direct insights into the technologies, challenges, and priorities of developers working in the cloud, edge, and IoT space.

II. Key Government & Policy Documents

These documents represent the official political and legal agenda and decisions, from high-level declarations to specific national laws and parliamentary reports.

Communication on the 2030 Digital Compass: the European way for the Digital Decade (European Commission, 2021)

Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0118

Relevance: Outlines the EU's high-level digital ambitions and targets for the decade, providing the strategic backdrop for the push towards digital sovereignty.

The Strasbourg Declaration: Guiding principles of a European vision for the digital space (The Government of France, 2022)

Source: https://france2022.fr/wp-content/uploads/2022/02/PFUE-Declaration-de-Strasbourg-EN.pdf

Relevance: A political declaration outlining a shared European commitment to developing digital technologies and infrastructure aligned with European values.

Strategy for Strengthening Digital Sovereignty for Public Administration IT in Germany (Federal Ministry of the Interior and Community, Germany, 2021)

Source: https://www.it-planungsrat.de/fileadmin/it-planungsrat/foederale-zusammenarbeit/Gremien/AG_Cloud/20210104_Strategy_for_strengthening_the_digital_sovereignty_of_public_administration_IT_1.0.pdf

Relevance: Outlines Germany's national strategy, emphasizing the central role of Open Source and open standards in achieving digital sovereignty for public services.

Bilanz von drei Jahren Digitalpolitik: WUMMS für digitale Abhängigkeit und Erpressbarkeit – Verlust der Glaubwürdigkeit (GI, 2024)

Source: https://gi.de/fileadmin/GI/Hauptseite/Aktuelles/Meldungen_und_Blogbeitraege/2024/2024-12-18-Bilanz-Digitalpolitik.pdf

Relevance: This article reports on a critical assessment by the German Informatics Society (GI) that highlights Germany's failure to meet its own Open Source and digital sovereignty goals, providing stark figures on the low level of Open Source procurement.

Studie zu Open-Source-Alternativen von Microsoft Services und Produkten in der Schweizerischen Bundesverwaltung (Standtke, R. & Tiede, M., Berner Fachhochschule, 2024)

Source: https://www.bk.admin.ch/dam/bk/de/dokumente/dti/themen/CEBA/studie-zu-open-source-alternativen-von-microsoft-services-und-produkten-in-der-schweizerischen-bundesverwaltung-backend-services.pdf.download.pdf/Studie%20zu%20Open-Source-Alternativen%20von%20Microsoft%20Services%20und%20Produkten%20in%20der%20Schweizerischen%20Bundesverwaltung%20Backend-Services.pdf

Relevance: A concrete, in-depth analysis commissioned by the Swiss Federal Administration, serving as a powerful case study for migrating public sector IT from proprietary to Open Source solutions.

Rapport d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne » (Latombe, P., Assemblée Nationale, France, 2021)

Source: https://www2.assemblee-nationale.fr/15/missions-d-information/missions-d-information-de-la-conference-des-presidents/souverainete-numerique-nationale-et-europeenne/(block)/RapportsInfoParlementairesInstance

Relevance: A key French parliamentary report that extensively analyses digital sovereignty and explicitly recommends prioritising the use of Open Source software (logiciel libre) in public procurement as a core pillar of national and European strategy.

Report on European technological sovereignty and digital infrastructure (Knafo, S., European Parliament, 2025)

Source: https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.html

Relevance: An own-initiative report from the Parliament's Committee on Industry, Research and Energy that analyses the EU's strategic dependencies across the entire digital value chain and proposes comprehensive measures to strengthen European technological sovereignty, including a focus on procurement and industrial policy.

III. Digital Sovereignty, Competition & Extraterritorial Risks

These sources outline the strategic thinking behind digital sovereignty and provide evidence of the specific legal and geopolitical risks posed by foreign legislation.

European Commission's use of Microsoft 365 infringes data protection law for EU institutions and bodies (EDPS, 2024)

Source: https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/european-commissions-use-microsoft-365-infringes-data-protection-law-eu-institutions-and-bodies_en

Relevance: A landmark legal decision demonstrating the sovereignty risks of dependency on a single non-EU vendor, even when data is hosted in Europe.

Cloud Sovereignty and the GDPR, Part One: US Government Access to European Data (Michels, J. D., Millard, C., Walden, I., & Wuermeling, U., 2024)

Source: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4911552

Relevance: This academic paper provides a detailed legal analysis of the conflict between US government access laws (like the CLOUD Act and FISA) and the GDPR, examining the specific compliance challenges and risks for European organisations using US cloud providers.

The EU-US "Data Privacy Framework": A wolf in sheep's clothing? (Max Schrems, 2023)

Source: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4329613

Relevance: Critiques the EU-US data transfer framework, highlighting risks that reinforce the report's argument for European-controlled infrastructure to uphold GDPR and data sovereignty.

Rapport d'information sur l'extraterritorialité de la législation américaine (Assemblée Nationale, France, 2016)

Source: https://www.assemblee-nationale.fr/14/rap-info/i4082.asp

Relevance: An official French parliamentary report detailing the risks and impact of US extraterritorial laws, providing a strong justification for seeking technological independence.

L'extraterritorialité du droit américain : un levier de domination économique mondiale (Calypso Hugon, 2025)

URL: https://www.portail-ie.fr/univers/2025/lextraterritorialite-du-droit-americain/

Relevance: This analysis frames US extraterritoriality as a tool of economic power, reinforcing the argument that technological dependence has direct geopolitical consequences.

Digital Sovereignty: Status Quo and Perspectives (Kagermann, H., Streibich, K.-H., & Suder, K., acatech, 2021)

Source: https://www.acatech.de/publikation/digitale-souveraenitaet-status-quo-und-handlungsfelder/download-pdf/?lang=en

Relevance: This foundational report from the German National Academy of Science and Engineering provides a technology layer model for analysing digital sovereignty, offering a structured framework for policy action.

L'Europe reste-t-elle une "colonie numérique" des États-Unis? (Nocetti, J., Politique étrangère, 2021)

Source: https://www.cairn.info/revue-politique-etrangere-2021-3-page-51.htm

Relevance: This journal article offers a high-level geopolitical analysis of Europe's technological dependency, framing the rise of digital sovereignty as a response to the "digital colony" status.

Avis n° 23-A-08 du 29 juin 2023 portant sur le fonctionnement concurrentiel de l'informatique en nuage ("cloud") (Autorité de la concurrence, France, 2023)

Source: https://www.autoritedelaconcurrence.fr/fr/avis/portant-sur-le-fonctionnement-concurrentiel-de-linformatique-en-nuage-cloud

Relevance: This official report from a major national regulator details the anti-competitive practices in the cloud market, justifying the need for sovereign, interoperable alternatives.

La guerre du cloud doit avoir lieu! (Fouilland, R., & Galas, G., La Gazette de la Société et des Techniques, 2023)

Source: https://annales.org/gazette/2023/Gazette_122_05_23.pdf

Relevance: This article, based on a research paper from the Corps des Mines, analyses the economic and geostrategic stakes of cloud sovereignty in Europe. It highlights the dominance of US hyperscalers and proposes concrete economic levers, including the promotion of Open Source solutions, to strengthen the European ecosystem.

IV. The Cloud, Edge & IoT Ecosystem: Strategy & Initiatives

These references provide specific context on the cloud, edge, and IoT domains, highlighting market failures, developer priorities, and key European-led alternatives.

European Industrial Technology Roadmap for the Next-generation Cloud-Edge (European Alliance for Industrial Data, Edge and Cloud, 2023)

Source: https://ec.europa.eu/newsroom/dae/redirection/document/102590

Relevance: This is the precursor roadmap from the Cloud-Edge Alliance, providing the high-level context from which this Open Source thematic roadmap is derived.

Next Generation Internet (NGI) Initiative (European Commission)

Source: https://digital-strategy.ec.europa.eu/en/policies/next-generation-internet-initiative

Relevance: The official source for the EU's flagship initiative for funding and developing a more human-centric, open, and sovereign internet.

Deploying the EuroStack: What's Needed Now. (EuroStack Initiative, written by Cristina Caffarra et al., 2025)

Source: https://eurostack.eu/the-white-paper/

Relevance: A concrete policy proposal that operationalises the roadmap's vision through three actionable pillars: 'Buy European' (procurement), 'Sell European' (market visibility), and 'Fund European' (investment strategies).

Sovereign Cloud Stack (SCS) Documentation and Vision (SCS Community)

Source: https://scs.community/

Relevance: A key practical example of a European-governed Open Source initiative aimed at building a standardised, sovereign cloud infrastructure, as referenced in the roadmap.

Position Paper: A Structured Framework for Europe's Digital Sovereignty: Technological Building Blocks for the Public Digital Infrastructure and Internet Commons (Fermigier, S., 2025)

Source: https://euro-stack.com/blog/2025/5/tbb-for-open-internet-stack

Relevance: This paper proposes a foundational taxonomy, the Technological Building Blocks (TBBs) framework, to structure and analyse the components of Europe's digital infrastructure, providing an essential analytical tool for implementing sovereignty policies.

V. Implementation: Public Procurement & National Strategies

These documents serve as concrete examples of the legal frameworks and policies advocated in the procurement pillar of the roadmap.

Strategy for Strengthening Digital Sovereignty for Public Administration IT in Germany (Federal Ministry of the Interior and Community, Germany, 2021)

Source: https://www.it-planungsrat.de/fileadmin/it-planungsrat/foederale-zusammenarbeit/Gremien/AG_Cloud/20210104_Strategy_for_strengthening_the_digital_sovereignty_of_public_administration_IT_1.0.pdf

Relevance: Outlines Germany's national strategy, emphasizing the central role of Open Source and open standards in achieving digital sovereignty for public services.

Gesetz zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften (OZG-Änderungsgesetz) (German Bundestag, 2024)

Source: https://www.recht.bund.de/bgbl/1/2024/245/VO.html

Relevance: This German law provides a powerful legal precedent by mandating a preference for Open Source software in public administration, demonstrating concrete policy action.

LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique (Loi Lemaire) (Gouvernement français, 2016)

Source: https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000033203039

Relevance: This is the landmark French law for the "Digital Republic" which, in its Article 16, explicitly mandates that public administrations should encourage the use of Open Source software

(logiciels libres) and open formats to ensure the control, longevity, and independence of their information systems.

Public Money, Public Code Initiative (Free Software Foundation Europe - FSFE)

Source: https://publiccode.eu/

Relevance: The foundational campaign advocating for the principle that publicly financed software should be made publicly available under a Free and Open Source Software license.

Socle Interministériel de Logiciels Libres (SILL) (DINUM, France)

Source: https://sill.etalab.gouv.fr/

Relevance: The official repository of recommended Open Source software for the French public administration—a primary example of a national evaluation and procurement guide.

Catalogo del Riuso (Software Catalogue) (Agency for Digital Italy & Department for Digital Transformation, Italy)

Source: https://developers.italia.it/it/software

Relevance: The Italian national catalogue of Open Source software for public administrations, another key example referenced in the roadmap.

VI. Implementation: Governance, Interoperability, Security & Community

These documents address the practical and legal frameworks necessary for building a mature, secure, and well-governed Open Source ecosystem.

The Cyber Resilience Act (European Commission)

Source: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

Relevance: The key legislative framework for cybersecurity requirements for products with digital elements, frequently referenced in the roadmap's governance and security pillars.

Europe's Open Source Industry's Statement on the Cyber Resilience Act (APELL, 2023)

Source: https://apell.info/2023/09/19/apell-statement-on-the-cra/

Relevance: This statement shows the direct impact of EU regulations on the Open Source ecosystem and underscores the importance of policy dialogue to avoid harming innovation and SMEs.

Some Thoughts on Interoperability (Stefane Fermigier, 2024)

Source: https://euro-stack.com/blog/2024/12/interoperability-thoughts

Relevance: This analysis explains the crucial difference between the strict, sovereignty-enabling definition of open standards in the European Interoperability Framework v1 (EIFv1) and weaker subsequent versions.

A Deep Dive Into Open Source Program Offices: Structure, Roles, Responsibilities, and Challenges (Haddad, Linux Foundation, 2022)

Source: https://www.linuxfoundation.org/research/a-deep-dive-into-open-source-program-offices

Relevance: This Linux Foundation guide provides the definitive model for the Open Source Program Office (OSPO), a key governance mechanism advocated for in the report.

Guidelines for Sustainable Open Source Communities in the Public Sector (Devenyi et al., European Commission, 2021)

Source: https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/guidelines-creating-sustainable-open-source-communities

Relevance: An official European Commission guide that offers a practical framework for public administrations to build and engage with Open Source communities, crucial for successful adoption.

ADEME Avis sur la soutenabilité environnementale du numérique (ADEME, 2025)

Source: https://librairie.ademe.fr/consommer-autrement/7883-avis-de-l-ademe-numerique-environnement-entre-opportunites-et-necessaire-sobriete.html

Relevance: Supports the roadmap's pillar on Environmental Sustainability by providing official analysis on the environmental impact of digital infrastructure.

Apports du logiciel libre à la durabilité des équipements (Conseil Logiciel Libre, 2023)

Source: https://code.gouv.fr/docs/2023_01_RapportIndiceDurabilite.pdf

Relevance: A focused report detailing the role of Open Source in promoting environmental sustainability and digital sobriety by extending the lifespan of hardware, a key theme of the roadmap.

ANNEX II: GLOSSARY

AI Act (Artificial Intelligence Act)

A landmark European Union regulation that establishes a harmonised legal framework for Artificial Intelligence. It takes a risk-based approach, imposing stricter obligations on AI systems deemed "high-risk" to ensure they are safe, transparent, and respect fundamental rights, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

API (Application Programming Interface)

A set of defined rules, protocols, and tools that allows different software applications to communicate and interact with each other. APIs are crucial for achieving interoperability between systems.

Cloud Computing

The on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centres and servers, organisations can access technology services, such as computing power, storage, and databases, from a cloud provider. Key models include IaaS, PaaS, and SaaS.

CRA (Cyber Resilience Act)

A European Union regulation establishing cybersecurity requirements for products with digital elements. It aims to ensure that hardware and software products are more secure, and it introduces specific responsibilities for manufacturers and stewards of Open Source software (https://eur-lex.europa.eu/eli/reg/2024/2847/oj).

Digital Sovereignty

The ability of a state, organisation, or individual to have autonomous control over their digital infrastructure, data, and technology, free from foreign or external coercion. It encompasses not only technological independence and data protection but also the capacity to align the digital environment with local laws, norms, and values.

Edge Computing

A distributed computing paradigm that brings computation and data storage closer to the data sources. This is done to improve response times, save bandwidth, and enable real-time processing, as opposed to sending data to a centralised cloud for processing.

Extraterritoriality

The legal principle allowing a state's laws to apply beyond its own borders, affecting foreign entities or data stored in other jurisdictions. A primary example is the U.S. CLOUD Act and FISA executive order, which is a major driver of the digital sovereignty debate in Europe.

F/OSS (Free and/or Open Source Software)

An inclusive umbrella term used to refer to software that is simultaneously Free Software and Open Source Software. It is often used interchangeably with FLOSS to denote the broad ecosystem of software that is not proprietary, without emphasizing the philosophical differences between the two movements.

FLOSS (Free/Libre and Open Source Software)

A widely used umbrella term that encompasses both Free Software and Open Source Software. The inclusion of "Libre" (from Spanish and French for "free") serves to clarify the meaning of "Free" as "freedom" (libre) rather than "at no cost" (gratis), resolving a common ambiguity in English.

Free Software

Software that grants users four essential freedoms, as defined by the Free Software Foundation (FSF). The focus is on the ethical and philosophical dimension of user freedom and control. The four freedoms are:

- Freedom 0: The freedom to run the program as you wish, for any purpose.
- Freedom 1: The freedom to study how the program works and change it so it does your computing as you wish. Access to the source code is a precondition for this.
- Freedom 2: The freedom to redistribute copies so you can help others.
- Freedom 3: The freedom to distribute copies of your modified versions to others.

If a program does not grant all four of these freedoms, it is considered proprietary, not Free Software.

GDPR (General Data Protection Regulation)

The cornerstone of the European Union's data protection and privacy legal framework. It regulates how personal data of individuals within the EU can be collected, processed, and stored, and grants specific rights to data subjects. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

IaaS (Infrastructure as a Service)

A fundamental cloud computing model where a provider hosts the core infrastructure components traditionally present in an on-premises data centre, including servers, storage, and networking hardware, as well as the virtualisation layer.

Interoperability

The ability of different computer systems, applications, or services to connect and communicate in a coordinated manner to exchange and make use of information. It allows systems to work together without special effort from the user, often enabled by adherence to open standards.

IoT (Internet of Things)

The network of interconnected physical devices ("things") embedded with sensors, software, and other technologies that allows them to connect and exchange data with other devices and systems over the Internet.

Open Source Software (OSS)

Software for which the original source code is made freely available and may be redistributed and modified. The term, promoted by the Open Source Initiative (OSI), emphasises the pragmatic benefits of a collaborative development model, such as reliability, peer review, and faster innovation, over the philosophical aspects of user freedom. The definition is based on a set of 10 criteria applied on the license's properties rather than the four essential freedoms in the Free Software Definition. In practice, both definitions should be considered equivalent.

Open Standards

Standards that are publicly available, developed and maintained through a collaborative and consensus-driven process, and which can be implemented without royalties or significant restrictions. They are essential for ensuring interoperability and preventing vendor lock-in.

OSPO (Open Source Program Office)

A designated centre of excellence within an organisation responsible for establishing and managing its Open Source strategy, policies, legal compliance, and community engagement.

PaaS (Platform as a Service)

A cloud computing model where a third-party provider delivers a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the underlying infrastructure.

Public Money, Public Code

A policy and advocacy campaign asserting that software paid for by the public sector should be made available to the public under a Free and Open Source license, allowing for inspection, reuse, and collaborative improvement.

SaaS (Software as a Service)

A software licensing and delivery model in which software is centrally hosted and licensed on a subscription basis. It is the most abstracted cloud model, where users access the software over the internet, typically via a web browser.

Vendor Lock-in

A situation in which a customer using a product or service becomes dependent on that vendor and cannot easily switch to a competitor without incurring substantial costs, effort, or data loss. This is often caused by proprietary technologies, incompatible data formats, and contractual restrictions.