Grant Agreement No.: 101135632 | **Call:** HORIZON-CL4-2023-DATA-01
Topic: HORIZON-CL4-2023-DATA-01-06 | **Type of action:** HORIZON-CSA

D3.3 Digital Policy Report - c

Revision: Final

Work package	WP3	Task	Task 3.1/3.2/3.3/3.4/3.5
Submission date	29/06/2026	Due date	30/06/2026
Deliverable lead	TECNALIA	Version	Final
Authors	Francesco Panella (Martel), Francisco Picolini (ONS), Andrew A. Adams (MEIJI), Tajana Medakovic, Danijel Pavlica (F6s), Sachiko Muto (RISE), Xabier Uriarte, Javier Mendibil, Juncal Alonso (TECNALIA),		
Reviewers	Thomas O. Timoudas (RISE), Alberto P. Martí (ONS)		

Abstract	This document presents the methodological framework to be followed in the Project for the monitoring and analysis of the European regulatory landscape and policy initiatives related to the Cognitive Computing Continuum. It is an ongoing deliverable with an initial version in M9, covering the description of the project approach and the initial EU policy and regulatory landscape analysis, and subsequent, updated versions produced in M18 and M30.
Keywords	Regulatory framework, policy, Open Source, standardisation, skills, digital sovereignty.

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V0.1	22/04/2026	1st version of the TOC for comments	Juncal Alonso (Tecnalia)
V0.2	30/04/2026	Agreed version of the TOC. Ready to start editing.	All
V0.3	29/05/2026	Contributions from the partners	Francesco Panella (Martel), Francisco Picolini (ONS), Andrew A. Adams (MEIJI), Tajana Medakovic, Danijel Pavlica (F6s), Sachiko Muto (RISE), Xabier Uriarte, Javier Mendibil, Juncal Alonso (TECNALIA)
V0.4	04/06/2026	Sent to internal reviewers	Juncal Alonso (Tecnalia)
V0.5	16/06/2026	Comments from reviewers	Thomas Olson (RISE)
V0.6	17/06/2026	Addressed comments from the reviewers	Juncal Alonso (Tecnalia), Sachiko Muto (RISE)
V0.7	18/06/2026	Sent to Management team	Juncal Alonso (Tecnalia)
V0.8	25/06/2026	Mgmt. review and addressing of final issues	Annika Strömdahl (RISE)
V1.0	29/0672026	Finalisation of deliverable	Juncal Alonso (Tecnalia)
Final	29/06/2026	Final deliverable for submission	Maria-Angeliki Evliati (RISE)

Disclaimer

Copyright notice

Project co-funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	R	
Dissemination Level		
PU	*Public, fully open, e.g. web*	**x**

Executive summary

Deliverable D3.3, the final "Digital Policy Report," provides a comprehensive strategic analysis of the policy and regulatory landscape surrounding the EU Cognitive Computing Continuum. As the culmination of a multi-stage project effort, this report aims to bridge the gap between technical innovation in Edge, Cloud, and IoT technologies and the regulatory frameworks required to ensure European digital sovereignty.

The report provides a dual-layered analysis. First, it maps the evolving European regulatory scene, identifying the instruments that impact the computing continuum. Second, it introduces a global dimension, offering comparative insights from Japan, the Republic of Korea, Canada, New Zealand, and India to identify international best practices and potential synergies for the EU. A critical component of this analysis is the exploration of Open Source (OS) and Open Standards, which are presented not merely as technical choices, but as strategic pillars for reducing vendor lock-in and enhancing technological autonomy. This is further illustrated through a maturity analysis comparing Open Source adoption in the Automotive and Agriculture sectors.

To translate these findings into action, the report employs a rigorous three-step methodology, Framework Setting, Implementation, and Refinement, to derive evidence-based policy recommendations. These are consolidated into seven strategic Policy Recommendations designed to unify fragmented infrastructure, strengthen trust in cross-border data fluidity, and support the scalability of European SMEs.

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

Table of content

List of figures

List of tables

Abbreviations

ADS	Agricultural Digital Solutions
AI	Artificial Intelligence
CEI	Cloud Edge and IoT
CRA	Cyber Resilience Act
DATS	Digital Agricultural Technologies
DMA	Digital Market Act
DSA	Digital Services Act
EECC	European Electronic Communications Code
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUCS	European Cybersecurity Certification Scheme for Cloud Services
EUDR	EU Deforestation Regulation
FLOSS	Free, Libre and Open Source Software
GDPR	General Data Protection Regulation
HE	Horizon Europe
HPC	High Performance Computing
IIoT	Industrial Internet of Things
IoT	Internet of Things
NGI	Next Generation Internet
OSH	Open Source Hardware
OSS	Open Source Software
PII	Personally Identifiable Information
ROK	Republic of Korea (aka South Korea)
SIP	Sustainable Innovation Pilots
SWOT	Strengths, Weaknesses, Opportunities, Threats
TWG	Thematic Working Group
VET	Vocational Education and Training
WP	Work Package

Co-funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

1. Introduction

Deliverable ***D3.3, "Digital Policy Report – c,"*** represents the culmination of a series of three strategic reports (M9, M18, and M30) designed to analyse and raise awareness within the European computing community regarding policy initiatives affecting the NexusForum.EU ecosystem.

This final report provides a comprehensive synthesis of the EU's policy and regulatory landscape within the context of the Cognitive Computing Continuum. Expanding beyond the European scope, this version also integrates international perspectives from key partners, including Japan, the Republic of Korea, Canada, New Zealand, and India. Furthermore, it examines the pivotal role of Open Source (OS) and Open Standards as essential pillars for enhancing European digital autonomy and technological sovereignty.

Drawing upon these analyses, D3.3 proposes a final set of policy recommendations structured around seven strategic **Policy Recommendations**:

- Unify fragmented infrastructure and integrate future technologies.
- Strengthen trust and cross-border data fluidity.
- Reduce vendor lock-in and strengthen strategic autonomy.
- Consolidate governance and coordination for the Continuum.
- Strengthen the Open Source and Standards commons.
- Support SMEs to scale and compete globally.
- Enhance technological sovereignty and adoption capacity.

These recommendations are derived from a rigorous methodological approach based on a SWOT analysis and the identification of 14 critical gaps, refined through iterative feedback from project stakeholders. The methodology followed a three-step process: Framework Setting (defining six critical factors influencing sovereignty), Implementation (identifying gaps in the Continuum), and Refinement (developing evidence-based policy recommendations with concrete technical implementation steps).

To facilitate dissemination, the report is complemented by a series of self-contained **Policy Briefs** available via the EUCEI webpage. These briefs cover international comparative analyses, extended SWOT analysis and the core Policy Recommendations graphical summary.

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

2. The EU Cognitive Computing Continuum: Final Policy & Regulatory landscape analysis

2.1 Comprehensive mapping of the European digital policy landscape

In previous NexusForum.EU deliverables [1] [2], the project conducted a comprehensive mapping of the European policy and regulatory landscape relevant to the Computing Continuum. This work resulted in the creation of a policy-to-technology framework that systematically analysed how European legal instruments, policy initiatives and strategic programmes influence the technological domains identified in the NexusForum.EU Research and Innovation Roadmap [3].

The analysis covered a broad range of legislative and policy measures, including data, cybersecurity, artificial intelligence, cloud, telecommunications, and digital infrastructure regulations, providing stakeholders with a structured view of the evolving European regulatory environment, as appears on Figure 1.

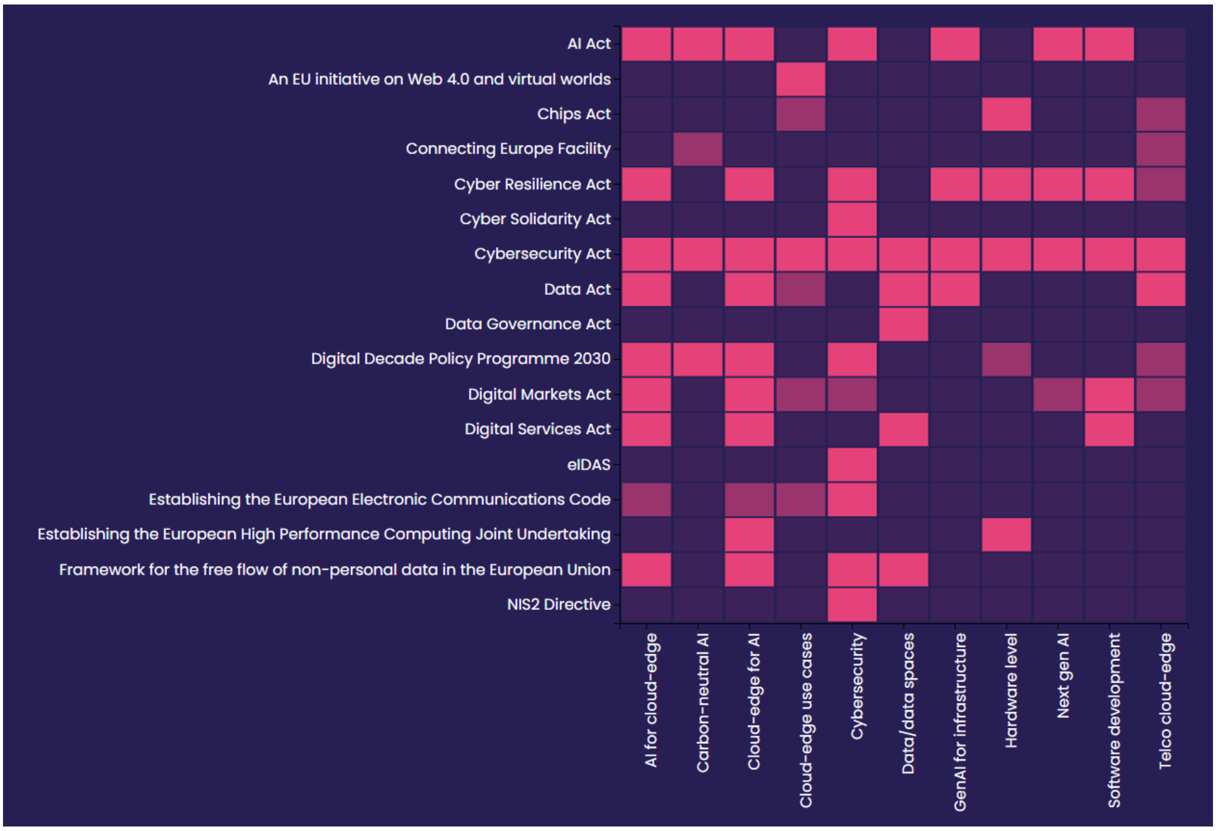

Figure 1 – Excerpt of the interactive policy matrix on the EUCloudEdgeIoT.eu website

The framework developed during previous reporting periods remains valid and continues to provide the basis for analysing the relationship between European policies and the technological addressed by the NexusForum.EU roadmap. We maintain this matrix as the reference structure for assessing policy impact across the various technological domains.

Building upon this foundation, the present report focuses on a new generation of policy initiatives that are currently under discussion, preparation or expected to enter the European legislative process in the coming years. They are expected to play a significant role in shaping the future European cloud-edge ecosystem, digital sovereignty objectives, and strategic technology capabilities.

2.2 Flagship strategies and policies on the European digital ecosystem

The following section provides an assessment of the most relevant upcoming policy instruments and strategic initiatives currently being developed at European level, examining their potential impact on the technology domains covered by the NexusForum.EU roadmap, and their relevance for the future evolution of the European Computing Continuum. These technology domains have been described in [3, 4, 5] and cover:

- **AI for Cloud-Edge**: Orchestration and Managing a Multi-Provider Continuum
- **Cloud-Edge for AI**: Enabling and Facilitating AI Applications Across the Continuum
- **Carbon-neutral AI**: Sustainable, energy-efficient, and energy-grid-aware Compute Continuum
- **Cloud-edge use cases**: Requirements from next-generation applications
- **Cybersecurity**: Security processes and controls in the cloud
- **Data/data spaces**: Access to European data, common data spaces, and data privacy
- GenAI for infrastructure: GenAI assisted operation and maintenance of Compute Continuum.
- **Hardware level**: EuroHPC, AI Factories and chips (RISC-V)
- **Next Gen AI**: Holistic AI (Gen AI and ML)
- **Software development**: Software development for the Compute Continuum or to be deployed on the Compute Continuum.
- **Telco cloud-edge**: Telco as the main tenant and implications for infrastructure providers

Several of these initiatives go beyond traditional regulatory objectives and seek to accelerate the deployment of strategic technologies, stimulate investment in digital infrastructures, foster industrial innovation, and support the development of sovereign European capabilities.

2.2.1 AI Continent action plan

Cloud-edge for AI

One of the key domains addressed by the AI Continent action plan (COM/2025/165 final) is computing infrastructure. Expanding the EU cloud and data centre capacity is essential to support the increasing deployment of AI solutions. The plan defines targets for the expansion of the European data centre capacity and supports the deployment of AI factories, with an aim to ensure researchers and businesses can have access to cutting-edge computation resources.

Data/data spaces

Data is one of the pillars of the action plan. On data, the action plan focusses on the delivery of a Data Union Strategy, published in late 2025 in the Communication COM(2025) 835 final[1]. The overarching objective is to unlock data for the development and deployment of AI solutions, supporting the work of European actors in the sector.

Next gen AI

The plan provides a roadmap to position Europe as a global leader in the AI sector by coordinating investments across infrastructure, data, skills, and regulatory simplification. By ensuring broad access to computational resources, the plan aims to support the creation of advanced AI technologies and foster Europe's technological sovereignty.

Software development

One of the overarching objectives of the plan is to ensure the European infrastructure and data environment are supportive to the development of the European AI ecosystem. This includes also software development, and the attempt to reduce barriers to the development and adoption of AI.

2.2.2 Competitiveness compass

Carbon-neutral AI

While not directly establishing a link between carbon-neutrality and artificial intelligence, the compass identifies decarbonising the economy as one of three transformational imperatives for EU competitiveness. The strategy emphasises the need for a joint decarbonisation and competitiveness plan to lower energy costs and thus avoiding hampering growth.

Cloud-edge for AI

The Competitiveness compass (COM/2025/30 final) identifies the need for cloud, data and infrastructure required for AI leadership. In this context, the document specifically outlines a plan of policy actions to ensure further advancement in the domain, namely by planning the development of the EU Cloud and AI Development Act, for which a “Proposal for the Cloud and AI Development Act, CADA”[2] has recently been adopted at the time of writing.

Hardware level

Reducing excessive dependencies and increasing security is one of the pillars of the compass, which highlights the need to improve the EU’s autonomy in the advanced technology supply chains.

The strategy, echoing the Draghi Report, highlights the need to *ensure the resilience of its supply chains, notably for critical raw materials, or imports of essential advanced clean or digital technologies, such as semiconductors.* This has been substantiated by the launch of

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0835

[2] Proposal for the Cloud and AI Development Act (CADA) | Shaping Europe’s digital future

Co-funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

the EU Energy and Raw Materials Platform, launched in July 2025, and by the Chips Act 2.0 proposal, presented in June 2026.

Next gen AI

The compass stresses that Europe must close its innovation gap by supporting the development of digital technologies including AI and quantum computing. The Competitiveness compass highlights the importance to support European endeavours on the development of AI technologies, and reporting on policy actions such as the AI Act, the AI Continent action plan, mentioned above and the EU Cloud and AI Development Act, for which a Proposal has been published by the European Commission in June 2026, also described below in this chapter.

Telco cloud-edge

The compass identifies some key actions with reference to the European digital infrastructure, specifically in the domain of telco cloud-edge. This encompasses the delivery of the EU Cloud and AI Development Act, introduced in the previous paragraph, and outlined below and the Digital Networks Act, adopted in its proposal form in January 2026. Additionally, the European Commission adopted a Proposal on the *procedure for authorisation of systems providing mobile satellite services using the harmonised 2 GHz*.

2.2.3 European Data Union Strategy

Data/data spaces

The strategy, working in tandem with horizontal legislation like the Data Act, establishes the essential framework to create a secure and interoperable single market for data across Europe. This unified data market is identified as the fundamental driver underpinning the broader development and deployment of AI. By laying these foundations, the strategy also guides the complementary development of a smart and secure middleware cloud platform dedicated to supporting common European data spaces. Ultimately, the strategy serves as one of the core policy pillars embedding the concept of "digital sovereignty" into the European digital economy, ensuring data is managed and shared under trusted conditions.

AI for cloud-edge

To ensure that these robust data environments translate into practical technological adoption, the strategy is designed to establish direct synergies with the newly established Experience and Acceleration Centres for AI (Centres for AI). By linking the data initiatives launched under the Data Union Strategy with these regional hubs, the EU aims to provide expertise and testing environments that facilitate the seamless integration of AI into strategic industrial sectors, thereby supporting the digital transformation of SMEs, small mid-caps, and public sector bodies.

2.2.4 Apply AI

The Apply AI strategy has been introduced as part of the broader European agenda to encourage the vertical integration of AI solutions across European industries.

AI for Cloud-Edge and Cloud-Edge for AI: The Apply AI strategy directly supports the deployment of AI solutions within cloud and edge environments. The initiative is expected to facilitate access to AI technologies, computing resources, and deployment environments, enabling organisations to integrate AI capabilities into cloud-edge infrastructures more effectively.

GenAI for Infrastructures, and NextGen AI: The strategy seeks to bridge the gap between European research and industrial adoption ('bridging the gap between research labs and deployment more effectively'). By fostering AI adoption across European industries, the Apply AI Strategy aims to create a European ecosystem capable of transforming AI research into operational solutions while promoting interoperability, trustworthiness, security and compliance with European regulatory frameworks.

2.2.5 Digital Sovereignty Package

In June 2026 the European Commission published the European Technological Sovereignty Package, a far-reaching set of measures aimed at fostering the European Union's digital autonomy. The package includes two legislative proposals, the *Chips Act 2.0* and the *Cloud and AI Development Act*, and two Communications, the *Communication on European Tech Sovereignty, accompanied by an EU Open Source Strategy* and the *Strategic Roadmap for Digitalisation and Artificial Intelligence (AI) in energy.*

The *Communication on European Tech Sovereignty,* and the *EU Open Source Strategy* propose a wide and high-level approach to technological sovereignty, giving the European open source ecosystem centre stage in the endeavour to improve the Bloc's technological autonomy.

The *Strategic Roadmap for Digitalisation and Artificial Intelligence (AI) in energy* aims at supporting the development of digital solutions which can help the European decarbonisation, while addressing the challenges posed by the growing energy demand stemming from AI deployment. Additionally, the Communication aims at supporting efforts on energy consumption optimisation.

The Chips Act 2.0 and the Cloud and AI Development Act clearly interact with some of the technology domains addressed by NexusForum.EU, and are therefore explored in the following sections.

Chips Act 2.0

In June 2026, the Commission published a Proposal for the Regulation known as Chips Act 2.0. The proposed act aims at supporting the European Union autonomy and security in supply chains of key semiconductors. The policy action aims at responding to quickly evolving needs, as well as tackling alleged limitations of the 2023 flagship Chips Act. The Proposal identifies three specific objectives, namely:

1. Enhance the capacity, security of supply and competitiveness of the EU semiconductor industry across the value chain, including leading-edge AI chips
2. Develop a strong user market across key industry sectors
3. Increase intelligence capabilities for crisis preparedness and response

Hardware level

The Chips Act 2.0 would introduce measures to support the European Union's chip making capabilities. This includes the objective to reduce excessive dependence of non-EU suppliers for critical semiconductor design and manufacturing, and supporting European production and development of semiconductors. To this end, the Proposal lists specific areas of intervention, including the *design capacities for integrated semiconductor technologies,* the continued operation of the *pilot lines for preparing for innovative production, testing and validation*, and the potential creation of new ones, should the need be identified, a specific focus on a*dvanced technology and engineering capacities for quantum chips,* continued support to the *network of semiconductor competence centres and skills development*, and potential launch of new ones or repurposing of existing ones, depending on market and technology development. *Advanced design, prototyping, and industrial deployment capacities for photonic integrated circuit technologies* will continue to be supported, with a specific focus on industrial uptake. Similarly, the *Chips Fund activities for access to capital by start-ups, scale-ups, and SMEs*, will continue, with a shift of focus towards scale-up operations.

CADA – Cloud and AI Development Act

The Cloud and AI Development Act (CADA) is an upcoming legislative initiative announced by the European Commission as part of the broader European Tech Sovereignty Package. The proposal is currently under discussion and is expected to progress through the legislative process during 2026. CADA is expected to provide greater legal clarity regarding sovereign cloud services, trusted providers, and strategic digital infrastructures, while supporting investment in cloud and AI computing capacity throughout Europe.

AI for Cloud-Edge: The initiative seeks to expand European computing capacity and facilitate access to the infrastructure required to develop, train, deploy and operate advanced AI systems. It may also contribute to the development of sovereign AI ecosystems capable of supporting strategic European sectors and public administrations.

Cloud-Edge for AI: CADA is expected to encourage the deployment of secure, high-performance infrastructure that can host advanced AI services while ensuring compliance with European requirements for security, data protection and sovereignty. The initiative may also facilitate the emergence of European cloud environments specifically designed to support AI workloads and highly critical use cases.

Data Spaces: This initiative expects to contribute to the creation of trustworthy cloud infrastructures, by promoting sovereign cloud services, trusted digital ecosystems, and greater computing capacity across Europe.

GenAI for Infrastructures: By supporting investment in Data Centres, cloud infrastructures, and AI computing capabilities, CADA could provide an enabling framework for the deployment of Generative AI services across Europe. Along with the possibility of developing a sovereign European AI models and platforms capable of operating within trusted infrastructures.

Telco Cloud-Edge: By supporting investments in digital infrastructures and sovereign cloud services, CADA may contribute to strengthening the foundations required for future 5G and 6G ecosystems.

2.2.6 Digital Omnibus on AI

The Digital Omnibus on AI is a proposed Regulation which aims at facilitating innovation in Europe. The proposal, if fully adopted into legislation, would introduce relevant changes in the application of rules on artificial intelligence as well as on data protection.

Software development

The Omnibus strongly focuses on reducing the administrative and compliance burden for software developers, with specific reference to the AI sector. It extends regulatory simplifications and reduces the compliance requirements for data access for AI training, including potential changes to the definition of personal data.

Data/data spaces

The proposed regulation would establish a specific legal basis that allows providers and deployers of AI systems and models to exceptionally process "special categories of personal data."

2.2.7 CSA2

In January 2026, the European Commission proposed a revision of the EU Cybersecurity Act as part of a broader Cybersecurity Package aimed at strengthening Europe’s cyber resilience. This proposal introduces a new Trusted ICT Supply Chain Framework, reforms the European Cybersecurity Certification Framework, and further strengthens the role of the European Union Agency for Cybersecurity (ENISA). The implementation is likely expected for 2027.

Cloud-Edge for AI: CSA2 introduces mechanisms aimed at assessing and mitigating risks originating from suppliers considered critical to the operation of essential infrastructures. The proposed framework could reinforce trust in sovereign cloud-edge environments and reduce dependencies on suppliers identified as presenting elevated security risks.

Telco Cloud-Edge: One of the most significant aspects of CSA2 concerns telecommunications infrastructure. The proposal explicitly addresses risks associated with suppliers of critical ICT assets and builds upon previous European efforts to secure 5G networks. The framework introduces the possibility of coordinated risk assessment and restrictions for suppliers considered high-risk in critical infrastructures.

Cybersecurity: The proposal expands ENISA’s mandate, strengthens incident response capabilities, introduces new vulnerability management mechanisms, improves cybersecurity certification processes, and establishes a trusted ICT supply-chain framework for critical sectors. The initiative seeks to facilitate compliance with existing European cybersecurity legislation while improving coordination among Member States.

Software Development: The CSA2 is intended to improve coherence between NIS2, Cyber Resilience Act, and other cybersecurity legislation, potentially reducing regulatory fragmentation while reinforcing cybersecurity requirements across software ecosystems.

2.2.8 Quantum Act

In 2025, the European Commission announced its intention to develop a European Quantum Act as part of the broader Quantum Europe Strategy, which aims to position Europe as a global leader in Quantum technologies by 2030. The proposal is currently under preparation and is expected to be formally presented during 2026, with implementation likely extending into 2027 and beyond.

Cloud-Edge for AI, and AI for Cloud-Edge: Although quantum computing remains at an early stage of industrial deployment, its future integration with cloud and edge infrastructures is expected to create new opportunities for advanced AI workloads, optimization problems, simulation environments, and scientific computing applications. The Quantum Europe Strategy specifically highlights the need to develop quantum infrastructures that can be integrated with Europe’s broader digital ecosystem, including cloud, edge, high-performance computing, and artificial intelligence platforms. These developments may ultimately influence future cloud-edge architectures by introducing hybrid classical-quantum computing environments.

Co-funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

Cybersecurity: Quantum technologies are expected to have a significant impact on cybersecurity, particularly through the development of quantum-safe communications, quantum key distribution (QKD), and post-quantum cryptography. As quantum computing capabilities mature, organizations operating cloud, edge, and data infrastructure will increasingly need to consider quantum-resistant security approaches.

2.3 International perspectives in the Cognitive Computing Continuum policy landscape

This section explores concept of "pooled digital sovereignty" through international cooperation by analysing the Cognitive Computing Continuum policy landscape at international scale.

Section 2.3.1 outlines the selection criteria for the five focus countries, Canada, India, Japan, New Zealand, and the Republic of Korea, detailing the linguistic, regulatory, and strategic reasons for their inclusion. Section 2.3.2 then provides a comprehensive comparative analysis of these nations across the key pillars of the Cognitive Computing Continuum, including Cloud-Edge-IoT, AI, semiconductors, data spaces, and smart cities, concluding with the potential synergies and policy recommendations for the European Union.

2.3.1 Case studies: Japan, South Korea, Canada, New Zealand and India

The NexusForum.EU concept is that the EU should, in seeking to divest itself of an over-reliance on US hyperscalers, not seek to replace those with EU hyperscalers. Dependence on one or a small number of large commercial enterprises for mission- or safety- critical public sector IT provision, whether based in the same jurisdiction or not, creates an unacceptable political power base outside of democratic norms. The reliance of a large portion of a country's (or supra-national regions such as the EU) commercial and third sector enterprises on an oligopoly is similarly problematic. Hence the projects focus on interoperable, federated scalable services for the future development of the continuum, replacing hyperscaler cloud with a variety of companies large and small. The benefits of this approach within the EU are presented elsewhere in the project's deliverables.

The interoperable, federated approach offers an opportunity to not just replace EU's dependency on US hyperscalers, but to work with other countries to deploy systems which can provide strength in depth and strength in breadth without undermining any individual areas digital sovereignty. Inspired by the EU's core concept of pooled sovereignty this idea of pooled digital sovereignty would allow competition for business not just within the EU by and for EU-based entities, but across a broader set of countries, but avoiding becoming dependent on any country which backslides on the rule of law or privacy protections for citizens.

The project therefore sought to identify a suitable set of countries whose policy landscapes could be studied for such opportunities. Through a combination of factors, the countries chosen were Canada, India, Japan, New Zealand, and the Republic of Korea (aka South Korea). This choice was partly pragmatic: all the countries chosen provide their policy documents in English, Korean or Japanese, the languages most readily available to the project in this task. Canada, Japan, New Zealand, and the Republic of Korea are all now associated with Horizon Europe as international partners, and the expected influence of the Research and Innovation Roadmap (and the combination of the two) on future Horizon Europe (and Horizon Framework 10) research funding in the area of the continuum means that these countries' policy and research landscapes were important for the project. India's rise as one of the world's largest single democratic economies (albeit still a developing one when measured as GDP per capita) combined with growing trade links between India and the EU provided the impetus for its inclusion in the group of countries studied. All the countries studied either have GDPR equivalence rulings (all except India) or the potential to receive one (India has a fairly strong data protection regime and may consider alignment in future, possibly as part of a joint continuum development effort). Other countries/groups such as Mercosur deserve study, but the resource limitations of the project inhibited further expansion. A future project on the continuum should consider studies of Mercosur, African Union, and other Asian (e.g. Indonesia, Vietnam, Thailand, Malaysia) countries/regional groupings for a similar study.

2.3.2 International perspective: A comparative analysis

Background

The EU has a wide-ranging set of policies to promote productivity, national security, and human rights via its international digital strategy [1], building on its existing Digital Partnerships and Trade Agreements (many of which include digital cooperation elements). This will include both diplomacy aimed at strengthening and further developing digital governance approaches which are based on open infrastructure and interoperability. The European Union's governance, strategy and policy provisions on the digital economy and ecosystem are complex and far-reaching, ranging from data exchange and protection to industrial and technological sovereignty priorities to market regulation, to measure to increase competitiveness, to name but a few.

As noted in the various country-specific landscape analyses (see links in Annex) produced by the project, many countries, including but not limited to those considered, are concerned by their reliance in both the public and commercial sectors on US hyperscalers such as Microsoft, Google and Amazon. Many have started developing specific public sector policies around public sector data in cloud computing, requiring one or both of localisation of physical processing, nationally-owned private sector provision and/or increased publicly owned provision. In related areas such as AI research and innovation, and semiconductor design and fabrication, there is also investment and/or policy to increase national infrastructure and reduce reliance on US design and Taiwanese or other overseas fabrication (sometimes including providing incentives for overseas companies to be involved in the development of fabrication facilities). All the countries studied have invested or are continuing to invest in Smart City deployments but with limited attention being paid to the sovereignty issues this might raise. For those involved in Data Spaces development there is a similar variety of concerns, with acceleration of development often taking precedent over digital sovereignty concerns.

Cloud-Edge-IoT Policy

The European Union has several policies which apply to the cloud, edge and Internet of Things domains. This includes high-level policies touching upon the wider digital ecosystem, including flagship strategies such as the Digital Decade Policy Programme 2030, outlining the policy plan and priorities, the Competitiveness compass, outlining key areas of intervention to support European capacity to compete in a rapidly evolving global context. From a legislative perspective, as anticipated in the introductory paragraph of this chapter, the European Union has a comprehensive set of policies in place to regulate how the European digital ecosystem works. This includes, for instance, flagship policies on safety and cybersecurity such as the Cyber Resilience Act, the Cybersecurity Act, and the Digital Services Act ensuring from different perspectives that digitally enabled products and services made available in the European Union provide a good level of security and safety to the end-users. The European legislative corpus also includes provisions to ensure the correct functioning of the markets, with specific reference to measures on market competition, via the Digital Markets Act: this Regulation is particularly relevant for cloud services, as the provisions to support a fair competition in the market, have direct implications for the cloud ecosystem. Additionally, the European Union has specific regulations in place to define how data can be collected, transferred, stored and reused, which is particularly relevant for the three technology domains explored in this paragraph, with the key legislation on the matter being the Data Act and the Data Governance Act, regulating -from different perspectives- non-personal data exchanges and aimed at supporting a competitive data market and to establish conditions for the reuse of protected data, the General Data Protection Regulation, ensuring that a high level of protection of personal data is guaranteed for users located in the European Union. The coming months are expected to bring substantial evolutions to the European Union's strategy and regulatory landscape of the digital ecosystem, with particularly high expectations on simplification efforts, aimed at fostering the Bloc's competitiveness.

The Gaia-X initiative represents a pivotal effort by the EU to enhance digital sovereignty through the definition and implementation of federated cloud service protocols. Managed by the Brussels-based non-profit Gaia-X AISBL, the project has been subject to critique—most notably by Adler-Nissen & Eggeling [2]—for the involvement of US hyperscalers such as AWS, Microsoft, and Google in its Working Groups. While official policy states that only EU-based organizations can influence governance, membership continues to include the European subsidiaries of Microsoft, Google Cloud, and Huawei. Although it began as a Franco-German venture, Gaia-X has evolved into a global initiative with members from all countries examined in this project.

In a significant shift, non-European members (DSA Japan, IDRI RoK, and Digital Trust Canada) have recently been elected to the voter group of the Policy Rules Committee (PRC). The PRC's development of the Gaia-X Labels scheme has significantly shaped the EU's "Cloud Sovereignty Framework" [2]. This framework recently culminated in a tender allowing EU institutions and agencies to procure sovereign cloud services for up to €180 million over six years. The successful European bidders include Post Telecom (partnering with CleverCloud and OVHCloud), STACKIT, Scaleway, and a partnership between Clarence, Mistral and Proximus, led by Proximus using services from S3NS (a joint venture between Thales and Google Cloud).

Concerns about the processing of public sector data, particularly sensitive (e.g. national security, law enforcement, government finance) and PII (Personally Identifiable Information) on citizens/residents, are widespread, not just in the countries studied but worldwide (see the UN's Department of Economic and Social Affairs site on National Cloud Strategies for a compendium of many of these policies).

India seems to be the most advanced in adopting sovereign cloud for government processing, and has a general policy of expanding the Indian IT sector, but no specific policy on promoting national cloud use in the private sector. The Republic of Korea has a similar public sector regime to India, although something of a one-size fits all approach with less detailed evaluation of the risks for specific departments. Canada is heavily dependent on US hyperscalers, with some in-country provision to meet data localisation requirements. A major push to expand e-government may see further deployments on hyperscaler infrastructure, both in-country and internationally. New Zealand similarly relies heavily on US hyperscalers, with questions about digital sovereignty often responded to with concerns about economies of scale and efficient use of public money. A single large national cloud service provider is providing some competition in both the public and private sectors, boosted by contracts for government services requiring localised data storage/processing and NZ national ownership. Japan lags behind both in the deployment of cloud provision for government services (there is a major push underway to rapidly catch up on e-government) and in the development of policy or provision for government-run cloud or Japanese-owned public cloud provision.

In the Edge and IoT sectors, only the Republic of Korea has had a major push to develop home-grown Edge and IoT industries, in particular IIoT for the existing manufacturing base which provides much of the country's GDP. Japan's IT Promotion Agency (IPA) has recently published an initial set of proposals for a Cloud-Edge-IoT heavily influenced by the NexusForum.EU project's R&I Roadmap, seeking to regain some of Japan's recent loss of industrial manufacturing in high tech by promoting nationally-produced equipment for both the domestic and international markets. India is beginning to see mentions of a similar opportunity for manufacturing in Edge and IoT but has no significant policies in place to promote either core development or digital sovereignty in these areas. New Zealand and Canada seem to be missing any significant Edge and IoT strategies and policies at present, with government mention being limited to advice on security.

Artificial Intelligence Research, Innovation and Promotion Policy

The EU AI Office is already engaged with multiple overseas AI Safety Institutes, or equivalent [4]. This includes Japan and Republic of Korea as well as the UK and Australia. The recently expanded trade agreement between the EU and India also includes enhanced cooperation on ensuring the human-centred development of AI. The digital partnership with the Republic of Korea and recent moves there to stress trustworthy AI development, provides a grounding for cooperation to be enhanced in this area. The growing partnership with Canada, which also has an AI Safety Institute, should also provide a solid basis for cooperation. New Zealand lags far behind in this area with no publicly funded AI Safety Institute, only an NPO.

The opportunities for joint development of useful, sustainable and open AI models between the EU and Canada, Japan, Republic of Korea within the Horizon Europe programme, potentially including India as a specific allowed external partner, should be considered as a way of providing a counterbalance to the current US and Chinese dominance with proprietary models.

Semiconductor Design/Production Policy

EU cooperation with Japan and Republic of Korea on semiconductor design and fabrication is already in place in research and innovation. In addition, the EU is "committed to developing a dedicated programme that will facilitate talent exchanges and foster semiconductor skills among students and young professionals" with India [4]. Canada and New Zealand lack significant policies on semiconductor infrastructure. There is an opportunity to expand existing bi-lateral cooperation efforts to multi-lateral, and potentially an opportunity to engage Canada in these with some Canadian voices raising concern about the lack of a semiconductor policy in this area.

A focus on the open RISC-V and related architectures between the EU and these other countries could provide a solid knowledge base for chip and firmware design expertise, while joint funding of fabrication facilities gradually expanding to multiple countries could help address the current, concerning, bottleneck of Taiwanese manufacturing dominance which presents a geopolitical concentration risk, given the significant role of Taiwanese manufacturing.

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

Data Spaces Policy

Japan is one of the countries leading the development of Data Spaces, with its Data-EX group now also a member of the Gaia-X grouping. The Data-EX focus on open protocols and FLOSS (Free, Libre and Open Source Software) implementations is very much in tune with EU moves in this area and with the NexusForum.EU Research and Innovation Roadmap. The South Korean sectoral integration of data sharing may provide a useful partner in developing data space policies targeted to different sectors (health, education, industry) while the open protocols and infrastructure of the Japanese and EU collaboration could provide a drop-in replacement for the proprietary systems currently in use. India, Canada and New Zealand currently have little involvement in this area, which may be an opportunity for a ground-floor adoption push for the open approach being jointly developed by the EU and Japan, providing a commercial opportunity for Japanese and EU providers as well as cementing pooled digital sovereignty amid the shared approach to data protection of Canada and New Zealand (which both have GDPR adequacy as do Japan and the Republic of Korea). Concerns around the details of India's current data protection regime [2] are not necessarily a major barrier here, but a solid assessment of compatibility would be worthwhile, perhaps as a Horizon Europe project call seeking to provide a knowledge base on compatibilities and inconsistencies with a wider range of countries with whom digital trade is growing.

The European Union's common policy organisation on data spaces stems from the 2020 European Strategy for Data, which laid basis for the Data Act and harmonised the governance of Common European Data Spaces. Currently Common European Data Spaces exist for agriculture, cultural heritage, energy, finance, environmental sustainability, health, manufacturing, language, media, mobility as well as data spaces dedicated to public administrations, research and innovation, skills and tourism.

Smart City Policy

All of the countries studied had invested in smart city pilots and developments, with New Zealand being the weakest here. Further large scale investments in the Republic of Korea and Japan seem most likely to be fruitful for the joint development of open infrastructure (Cloud-Edge-IoT hardware, as well as AI and other software) and EU collaboration may be possible, although both countries are looking to local deployments to kick-start export potentials, so a careful approach will be needed on the business model aspects. India and Canada have had substantial prior investment in Smart Cities but this seems to be now coasting on momentum only without significant new funding or policies.

Open Smart City technology could be a very useful area of focus for innovation activity in Horizon Europe and successor framework program that could engage Japanese and South Korean partners.

At an EU level, the smart cities strategy revolves around several lines of action and policy documents. The latest Commission Communication directly targeting Smart Cities is the 2025 Communication 'An EU Agenda for Cities: Driving Growth and Prosperity', which identifies specific tools and actions including the Smart Cities Marketplace, the Horizon Europe-funded EU Mission on Climate-Neutral and Smart Cities, aligning to the United Nations's Sustainable Development Goal 11 'Make cities and human settlements inclusive, safe, resilient and sustainable', translated to the European context via the Joint Research Centre's European Handbook for SDG Voluntary Local Reviews. Additionally, the Citiverse European Digital Infrastructure Consortium (EDIC) has been established, with an aim to foster an ecosystem of digital solutions and services, leveraging in particular, data, digital twins, artificial intelligence, augmented/virtual reality towards improving urban living and sustainability. These objectives also interact with the EU Local Digital Twins Toolbox: a flagship initiative of the European

Commission aimed at providing a '[modular, standards-based suite of tools designed to help cities and communities across Europe simulate, analyse, and plan urban environments more effectively]().' Finally, yet importantly, the European Data Space for Smart Cities and Communities, aiming at creating a cross-sectorial data space for smart communities.

Digital Sovereignty Policy

In the last few years, the European Union has been increasing its efforts to increase its strategic autonomy and sovereignty, with specific reference to the digital ecosystem. From a high-level perspective, this follows different key directions, on the one side through actions to increase the bloc's competitiveness, as anticipated in the introduction to this chapter, and on the other side through tailored strategic, policy and funding initiatives supporting the development of a stronger, more cohesive and integrated European digital ecosystem. The concept of 'digital sovereignty' is embedded, more or less explicitly in several policies and strategies at EU level, including the AI Act, the AI Continent Action Plan, the Apply AI Strategy, the Chips Act, the Quantum Europe Strategy, the proposed Digital Networks Act, the Data Act, and the Data Union Strategy, covering a wide range of facets of the European digital ecosystem and economy. Finally, yet importantly, the Commission has recently introduced the Tech Sovereignty package, which includes the Strategic Roadmap for Digitalisation and AI in Energy, the Communication on European Tech Sovereignty, the Cloud and AI Development Act and the Chips Act 2.

The EU is engaged quite broadly in promoting mutual technological compatibility and legal recognition of electronic signature systems, including Japan and India [4]. This will enhance cooperation and mutual support in areas of Digital Public Infrastructure, a key area of development in all the countries studied, closely related to avoiding lock-in to hyperscalers (particularly US and Chinese companies) for critical national infrastructure. Joint development of pooled digital sovereignty across the broad range of Continuum platforms and protocols can use this approach as a guideline.

India, Canada and the Republic of Korea all have strong voices, sometimes within the current government (the Canadian and Indian Prime Ministers) as well as from many other legislators and third sector voices (digital rights activists in particular). Japan and New Zealand have fewer such voices generating wide public debate, although they do exist in those countries as well. The diverse moves towards digital sovereignty, often starting with public systems such as e-government and internal government processing, can be leveraged into a pooled digital sovereignty agreement supported by open protocols, FLOSS and Open Hardware, but this requires sustained policy and diplomatic effort.

Impact and potential synergies for the EU Cognitive Computing Continuum

The European Commission should undertake a similar policy review of other countries such as the Mercosur members to identify further possible partners for a common development of federated, open, pooled digital sovereignty systems, particularly where existing or under-negotiation free trade agreements would provide a solid basis for allowing service provision across borders without vendor or country lock-in. The economies of scale achievable by expanding both the providers and users of such services beyond the EU would provide strength in depth against individual countries becoming unreliable partners, while counterbalancing US and Chinese economies of scale from their hyperscaler providers.

The four Horizon Europe global associated countries (Canada, Japan, New Zealand and Republic of Korea) should be closely consulted on the direction of research and innovation funding in this area, with a focus on those areas which are relevant to implementing the digital sovereignty policy. Where possible, direct policy coordination to ensure that the results of Horizon Europe projects and other bi-lateral or multi-lateral technology research and innovation programs undertaken by the EU or EU Member states, whether involving partners from the global associated countries or not, should be undertaken by the Commission. Calls for proposals implementing these policy approaches would ideally promote or even require partners from the global association countries to be involved to ensure technical and policy compatibility, and to increase the likelihood of implementation in the non-EU partner countries.

Future projects in the Continuum, in Horizon Europe and the successor framework program, should be required to include representation from the global association countries to ensure a pooled digital sovereignty approach is at the heart of the technological developments undertaken.

Alignment with India, Japan and the Republic of Korea on semiconductor policy should be pursued by the Commission. There is a significant window of opportunity for avoiding future single points of failure (like the example in section "Semiconductor Design/Production Policy") by combining joint expertise in design and fabrication with a push for open design principles. Bilateral or multi-lateral programs for development of fabrication facilities will be more difficult to agree but may be possible.

Suitable non-profit governance arrangements for FLOSS and Open Hardware need support in research and innovation from Horizon Europe or direct Commission support. A majority of the current FLOSS projects underpinning development are currently based in the US, subject to US jurisdiction and vulnerable to capture by US commercial and government interests. Forking major FLOSS projects without suitable institutional infrastructure at best holds back development and at worst fails, leaving a captured body in charge of a major piece of soft infrastructure. Providing easier ways to create EU-based non-profits with international collaboration but without the risk of US or Chinese dominance should be a key policy goal. The Document Foundation, the German nonprofit which develops the LibreOffice suite provides a solid example of an EU-based but internationally open organisation. Preferential inclusion of such organisations in calls for relevant Horizon Europe, and future research frameworks, should be considered to ensure convergence between institutional development roadmaps and funded research and innovation goals. Education and training materials for FLOSS and Open Hardware, and the development of certifications for engineering excellence in these topics, are also areas that could be prioritised in the research and innovation frameworks and jointly developed with suitable partner countries.

The current era of shared concern over US and Chinese dominance in the digital field presents a strong opportunity for development of a new way forward, based on EU concepts of pooled sovereignty and human rights. In addition to funding the core open technological platforms and protocols, the internal policies of the EU need to prioritise public use of such systems by the EU and Member States' government, and international diplomacy aimed at sharing both the burdens and the benefits with like-minded international partners.

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

3. Increasing the awareness and participation in policy initiatives of the Cognitive Computing Continuum

NexusForum.EU contributed to strengthening stakeholder awareness and participation in European digital policy processes related to the Cognitive Computing Continuum. Through a combination of public consultation monitoring, community engagement activities, webinars, Working Group discussions, and international events, the project facilitated structured interaction between policymakers, researchers, industry representatives, and innovation actors.

The activities carried out during the last period of the project focused on increasing understanding of how European digital legislation and policy initiatives influence the development of cloud-edge infrastructures, artificial intelligence, cybersecurity, interoperability, data governance, and digital sovereignty. Particular attention was given to ensuring that technical and research communities – often underrepresented in policymaking processes – were informed about opportunities to contribute to European Commission consultations and strategic discussions.

The project also strengthened its role as a neutral ecosystem facilitator, creating spaces for dialogue between different stakeholder categories and supporting the translation of technical expertise and operational challenges into policy-relevant recommendations. Awareness and capacity-building activities included webinars, consultation workshops, roundtable discussions, policy-focused sessions, dissemination campaigns, and dedicated community engagements through the NexusForum.EU digital channels and stakeholder ecosystem.

The project also encouraged active participation in European policymaking processes by promoting European Commission "*Have Your Say*" consultations and facilitating dialogue between technical communities and policy actors.

3.1 Review of public consultation activities

NexusForum.EU actively monitored and promoted European Commission public consultation opportunities relevant to the Cognitive Computing Continuum. This included policy initiatives connected to AI, cloud and edge infrastructures, cybersecurity, interoperability, digital sovereignty, data governance, and emerging digital technologies.

A major activity under this effort was the organisation of the webinar "**How to Engage in EU Public Consultations – A Practical Guide for First-Time Participants**", held on 25 March 2026 and organised by F6S, ONS and TECNALIA. The webinar addressed the limited participation of technical and research communities in EU policymaking processes, despite the increasing regulatory impact of initiatives such as the AI Act, Digital Services Act, Data Act, and Cyber Resilience Act.

The webinar provided an overview of the European Commission's public consultation mechanisms, practical guidance on how organisations can contribute effectively, and examples of how legislation impacts the Cloud–Edge–AI ecosystem. Moreover, it provided insights into the importance of stakeholder participation in shaping future European policy and funding priorities. The activity also highlighted NexusForum.EU's role in facilitating structured stakeholder engagement and increasing awareness of participatory opportunities within the European digital policy landscape.

Co-funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

Beyond the webinar, the project continuously disseminated relevant consultation opportunities through its Community Forum, Working Groups, mailing lists, and social media channels, encouraging ecosystem actors to engage more actively in policy discussions and contribute technical perspectives to future legislative and strategic initiatives.

3.2 Analysis of stakeholder feedback from the NexusForum.EU community

Stakeholder engagement activities conducted throughout the reporting period generated substantial feedback and interaction from the NexusForum.EU community, which by the end of the reporting period consisted of **more than 120 onboarded members** representing research organisations, industry actors, startups, SMEs, policymakers, universities, and innovation ecosystem stakeholders across Europe and internationally.

Feedback and contributions were collected through multiple participatory activities, including:

- NexusForum.EU Working Group meetings and webinars;
- policy-oriented discussions and roundtables;
- the Community Forum hosted on the Whaller platform;
- surveys and roadmap validation activities;
- international workshops and events, including the EU–ROK Digital Convergence Week;
- bilateral stakeholder exchanges and networking sessions.

Stakeholders engaged across a broad range of thematic domains relevant to the Cognitive Computing Continuum, particularly AI and trustworthy AI systems, cloud-edge interoperability, cybersecurity and digital resilience, as well as open source and digital sovereignty, semiconductors and advanced computing, 6G and future networks, and quantum technologies.

The feedback received demonstrated interest in improving interoperability across European infrastructures, strengthening trusted and sovereign digital ecosystems, and reducing fragmentation across standards and initiatives. Moreover, the community showed interest in increasing collaboration between research, industry, and policymakers, as well as supporting clearer alignment between policy frameworks and technological realities. The participatory activities also highlighted the importance of international cooperation, particularly with strategic partners such as Japan and the Republic of Korea, and reinforced stakeholder demand for stronger cross-border research and innovation collaboration.

3.3 Impact of participatory actions on policy recommendations

The participatory actions implemented throughout the project had a direct impact on the development and refinement of NexusForum.EU's policy recommendations and strategic outputs.

Insights gathered through Working Groups, community discussions, webinars, workshops, surveys, and international events contributed to identifying key technological, regulatory, and operational challenges affecting the Cognitive Computing Continuum. These activities enabled NexusForum.EU to incorporate perspectives from a diverse stakeholder base spanning research, industry, startups, infrastructure providers, and policymakers. Stakeholder feedback significantly influenced recommendations related to digital sovereignty and trusted European infrastructures; interoperability and federated cloud-edge ecosystems; secure and resilient AI deployment; open source adoption and transparency; cybersecurity readiness and post-quantum preparedness; and future investment priorities for AI, cloud, edge, semiconductors, and quantum technologies.

The participatory process also reinforced the need for stronger alignment between policy objectives and real-world implementation challenges, particularly regarding compliance burdens, infrastructure fragmentation, standardisation gaps, and cross-border collaboration mechanisms. Importantly, the activities helped validate the relevance of the NexusForum.EU Research & Innovation Roadmap and Digital Policy Report by ensuring that recommendations were grounded in stakeholder expertise and ecosystem realities rather than developed solely from a top-down perspective.

4. Strategic analysis for digital autonomy: the role of Open Source, standards, and skills

Open source software has moved, in the space of a few years, from a question of cost and innovation to one of strategic autonomy. The European Commission's Communication on European Tech Sovereignty and the accompanying EU Open Source Strategy of 3 June 2026 frames open source as a key lever for reducing the dependence on non-EU providers and for securing the transparency, auditability and control on which both security and sovereignty rest. Section 4.1 examines what that ambition means in practice, and where Europe is well placed, or still exposed, to pursue it across the digital stack.

In section 4.2 the analysis then turns to the conditions that determine whether open source can deliver on this promise. It considers the increasingly close relationship between open source, standardisation, security and regulation – from the integration of open source communities into the work of the European standardisation organisations, to the formal standing given to open source stewards under the Cyber Resilience Act, and the implementing standards required by instruments such as the CRA and the AI Act. Taken together, these developments show open source being drawn from the margins of EU digital policy towards its core, with corresponding implications for funding, governance and the sustainability of shared infrastructure.

Because the Open Source Strategy operates at a deliberately horizontal level while value is created in specific sectors, section 4.3 grounds these themes in a vertical case study: open source in European agriculture. Compared to the more mature engagement of the automotive sector, the agricultural case illustrates the dynamics that shape open source's prospects in any domain – vendor lock-in and digital sovereignty, regulation as a driver of adoption (notably the EU Deforestation Regulation and the Data Act), the central role of foundations such as AgStack in sustaining outputs beyond project funding, and the persistent challenges of skills, fragmentation and long-term maintenance. It thereby shows why high-level EU policy has to translate into practical change on the ground, in the sectors where open source is actually adopted.

4.1 Open Source as a pillar of European digital sovereignty

The European Commission has recognised open source as an enabler of digital sovereignty for some time. That recognition can be traced at least to the Commission's 2021 study on the economic impact of open source software and hardware[3], which already moved the debate beyond cost and innovation towards autonomy. The study estimated that EU companies invested in the order of €1 billion in open source software in 2018, generating an economic impact of roughly €65-95 billion, and that a 10% increase in code contributions would add some 0.4-0.6% to GDP each year alongside hundreds of new ICT start-ups. Crucially for the sovereignty argument, it found that procuring open source rather than proprietary software allows the public sector to lower its total cost of ownership, avoid vendor lock-in, and thereby strengthen its digital autonomy.

[3] *Study about the impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy | Shaping Europe's digital future*

What was an emerging theme in 2021 has now been amplified and placed at the centre of EU policy. With the Communication on European Tech Sovereignty and the accompanying EU Open Source Strategy of 3 June 2026, open source is named as one of four interlinked initiatives of the Technological Sovereignty Package – alongside the Chips Act 2.0, the Cloud and AI Development Act (CADA), and the energy roadmap – and is described explicitly as a key lever for achieving the Union's technological sovereignty. The Communication is motivated by the Union's structural reliance on non-EU providers for the great majority of its digital products, services and infrastructure, and the spending of an estimated €264 billion a year on predominantly non-European proprietary IT. Open source is presented as the path that lets Europe reduce those dependencies, mitigate lock-in, and gain the transparency and auditability on which both security and sovereignty rest.

Europe is well placed to take this path, though not evenly so. The mapping of dependencies across the stack describes three contrasting situations: genuine strength in the middle layers – internet technologies, enterprise software such as CRM, ERP and collaboration tools, and parts of cybersecurity – where strong EU communities contribute to both global and home-grown projects; areas of moderate presence such as cloud and AI infrastructure and models, where EU actors exist but neither market share nor global contribution matches the available solutions; and areas of minor presence and critical dependency, notably semiconductors and EDA tools and consumer-facing applications like desktop and mobile operating systems, browsers and search. As the birthplace of Linux and home to a community of several million contributors, Europe has the talent and the codebase; what it has lacked is sustained funding, scale, brand recognition, and procurement routes that let open source compete on equal terms. The Strategy responds with a combination of supply-side measures – to help EU communities and companies develop, scale, maintain and secure high-quality components – and demand-side measures to accelerate adoption across the public and private sectors, organised around four objectives: leveraging open source for sovereignty; strengthening a vibrant open source ecosystem; promoting open and interoperable digital ecosystems in public administrations; and reinforcing digital standards and international outreach.

The Strategy identifies the software stack supporting the European cloud-to-edge continuum – spanning the compute, connectivity, data and AI service layers – as a priority area in which open European alternatives should be built. That builds on substantial groundwork: more than €250 million has already been invested under Horizon Europe in next-generation cloud-edge components, meta-operating systems and IoT-edge platforms, explicitly to enable a compute continuum with strong, trustworthy capabilities at the edge and far edge.

While the Strategy deliberately operates at a general, horizontal level: it sets objectives, instruments and an open source-first posture for the stack as a whole. The opportunities, however, are increasingly vertical – in transport, health, agriculture, industry, energy and automotive – and the Strategy also points in this direction, from industrial collaboration platforms in automotive and rail to the mainstreaming of open source in the Apply AI calls across strategic sectors. The case study presented in this roadmap is intended to show what that vertical translation looks like in practice, and why the impetus created at EU level needs to trickle down to the sectors where value is actually created.

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

4.2 The synergy between Open Standards, security, and regulation

The relationship between open source and standardisation is not new to EU policy. As early as 2018, the Commission-funded study *Standards and Open Source: Bringing them together*[4] analysed how Standards Development Organisations (SDOs) and open source communities could work together, and proposed a roadmap for integrating those communities into the standard-setting process. That study built on a commitment the Commission had already made in its 2016 ICT standardisation priorities to support better integration of open source communities into SDO processes, and it set out concrete collaboration models – from open source as a source of reference implementations of standards, through to communities participating directly in, or feeding their results into, the formal standardisation work.

A series of recent instruments has drawn open source communities more deeply into standardisation and, in doing so, given their governance structures formal standing. The Cyber Resilience Act (CRA) is the clearest example: it introduces the concept of the open source software steward and recognises foundations as "stewards" of the projects they support, acknowledging their role in keeping shared infrastructure secure and reliable. By attaching defined responsibilities to that role, the CRA goes beyond describing the ecosystem to acting as a stimulus for the creation and strengthening of steward organisations.

The Open Source Strategy builds on this momentum rather than starting afresh. It observes that the pervasiveness of open source in cybersecurity, AI and internet technologies makes it essential that standardisation properly reflects what the communities are building, and that the foundational standardisation work required by laws such as the CRA and the AI Act needs the structural engagement of open source communities to deliver high-quality standards. Concretely, the Strategy commits – in the upcoming revision of the EU Standardisation Regulation – to better integrate open source processes and communities into standard setting, to create conditions for certain standards to be implemented in open source, and to ensure adequate funding, all in the service of greater legal certainty and the timely availability of standards that underpin EU law. It also envisages a European steward organisation that could serve as a structured channel for European implementation experience to feed into European and international standardisation. The Commission has funded the participation of open source contributors in the development of harmonised standards (for example through the Cyberstand.eu project) and has worked with the European standardisation organisations CEN, CENELEC and ETSI to bring those communities into the process. The Call for Evidence that fed the Strategy reinforced the direction, with companies and business associations reaching near-consensus on the centrality of standards and interoperability.

Security is the third strand that binds standards and regulation together. Because open source code is transparent and publicly auditable, it is a preferred approach for cybersecurity; but transparency is not the same as resilience, and much critical infrastructure depends on components maintained by under-resourced volunteers. The Strategy addresses this through a coherent set of measures anchored in the CRA: accelerating the voluntary security-attestation programmes foreseen under the Act, building (with ENISA's support) a list of critical

[4] *https://digital-strategy.ec.europa.eu/en/library/standards-and-open source-bringing-them-together*

and security-relevant open source dependencies on the basis of the CRA's dependency-analysis concept and Software Bills of Materials, and establishing an Open Source Maintenance Instrument to fund the upkeep and security of essential components – including the capacity to fork projects where continuity is at risk.

4.3 Case Study: Open Source in Agriculture

4.3.1 Introduction

In February 2025, the European Commission published its Vision for Agriculture and Food, setting out a strategic direction for a competitive, resilient, and future-oriented agri-food system. The Vision is explicit that food security and food sovereignty – Europe's ability to produce sufficient, safe, and affordable food on its own terms – remain a defining priority, one that must be pursued in parallel with the sector's environmental obligations. Digital technology appears throughout as a critical enabler of this dual ambition and the Commission has committed to launching a dedicated EU digital strategy for agriculture, aimed at supporting the transition to digital-ready farming.

Against this backdrop, the question of who owns and controls agricultural digital infrastructure is becoming a strategic concern. European agriculture faces a multitude of pressures: geopolitical instability disrupting supply chains, climate adaptation demands that require real-time data and modelling capabilities, an ambitious sustainability agenda that imposes new monitoring and reporting obligations, and chronic labour shortages accelerating demand for automation. The Vision's emphasis on food sovereignty adds a further dimension. As one practitioner consulted for this paper put it: there is "no money in agriculture" in the way there is in other sectors – meaning that the capital-intensive, long-cycle nature of farming limits the sector's ability to develop and sustain its own digital ecosystem. This creates a structural dependence on platforms and tools developed by actors whose interests are not always aligned with those of farmers or with European policy objectives around sovereignty, sustainability, and equity.

Open source software offers a different model. By enabling shared development of non-differentiating digital infrastructure, OSS can lower barriers to adoption, prevent lock-in, foster interoperability, and keep innovation accessible to actors who cannot afford proprietary alternatives. These properties are particularly relevant in agriculture, where the diversity of farm types, scales, and contexts makes bespoke proprietary solutions economically unviable for the majority.

This section investigates the current state and future potential of OSS in European agriculture. It is inspired by and structured in dialogue with a 2023 vision paper on OSS in the automotive industry (Linåker and Nummelin Carlberg, 2023), which explored how a traditional, hardware-centric industry is navigating the transition to software-defined systems. The case was deliberately chosen to contrast with the more mature engagement with OSS in the automotive sector. While agriculture shares many of automotive's structural characteristics – fragmented supply chains, safety-critical use cases, long asset lifecycles, and a historically hardware-first culture – but differs in its stakeholder structure, resource constraints, and the degree to which OSS practices have taken root.

The case study is structured around six themes: the current use and reuse of OSS in agriculture; the sector's capacity for strategic OSS engagement; the ecosystem structures that support or inhibit collaboration; the challenge of balancing collaboration and competition;

safety, data sovereignty, and trust; and the policy and infrastructure conditions needed to unlock OSS's full potential.

In addition to desk research drawing on published academic literature, EU project reports, and policy instruments, this case study also draws on a number of expert consultations. Where direct quotes from consultations are used, they are attributed generically to preserve respondent confidentiality. The approach is explicitly forward-looking: the goal is not a comprehensive audit of existing tools but a mapping of the opportunity space and an identification of the structural conditions that will determine whether that opportunity is realised.

Throughout, the paper draws comparisons with the automotive sector, where OSS maturity is meaningfully higher. These comparisons are intended to be diagnostic rather than aspirational: agriculture has its own structural logic, and OSS strategies that work in automotive may need significant adaptation to be applicable.

4.3.2 The Current State of OSS in Agriculture

OSS in agriculture is most developed in three domains: farm data management, remote sensing and geospatial analysis, and supply chain traceability. In each, open tools exist and are in active use – but coverage is patchy, integration is limited, and awareness among end users (particularly small and medium farms) is low.

Farm Management and Data Collection

FarmOS is the most mature open source farm management platform currently in wide use. A web-based application built on the Drupal framework, it provides modular support for planning, record-keeping, asset tracking, and data collection, including offline data entry via the FarmOS Field Kit mobile app. FarmOS is developed by a community of farmers, developers, researchers, and organisations – a governance model that reflects what a sustainable OSS project in agriculture could look like at scale. Its architecture has made it a reference point for several EU-funded projects exploring how open platforms can serve as shared infrastructure.

FarmBot represents a complementary model in open source hardware (OSH): a robotic platform for small-scale precision growing, controlled via a web interface and built on Arduino microcontrollers. Its significance lies less in its current deployment scale and more in its demonstration that the OSS model – transparency, modularity, community governance – can extend from software to the physical systems that agriculture depends on.

Remote Sensing and Geospatial Tools

The most significant cluster of open source activity in agriculture currently centres on geospatial monitoring, driven in large part by the EU Deforestation Regulation (EUDR). The regulation's requirement for plot-level geolocation and supply chain due diligence has catalysed the development of several open tools.

WHISP (What Is In That Plot?), developed by the Food and Agriculture Organization of the United Nations (FAO), is among the most technically advanced. It applies a convergence-of-evidence approach, cross-validating multiple datasets – including Global Forest Cover maps, RADD deforestation alerts, and Tropical Moist Forest data – to support preliminary EUDR due diligence. Critically, it is designed to be accessible to users without geospatial expertise, including smallholder farmers who can generate their own compliance evidence via mobile device. WHISP is complemented by FAO's broader AIM4Commodities initiative and the Open Foris suite of tools for field data collection and national forest monitoring.

The broader geospatial toolchain for EUDR compliance now includes FAO Ground, TerraTrac, INATrace, KoboCollect, QField, and GeoRoots.eu – many of which are open source or freely available. An emerging standard, the GeoID, enables anonymous, consistent identifiers to be assigned to plot polygons across different systems, addressing one of the core interoperability problems in supply chain traceability. The Forest Data Partnership, coordinated by the World Resources Institute (WRI) with support from USAID and the US Department of State, is building shared open data infrastructure at a global level.

Supply Chain Traceability

INATrace, an open source digital traceability platform, was developed specifically to address the economic situation of smallholder farmers by improving transparency in global commodity supply chains. By making value distribution visible at each stage of the supply chain, it both enables regulatory compliance and supports fairer trade practices. The platform has been adopted in several agricultural commodities and is being integrated into the AgStack infrastructure.

The December 2025 announcement of 'Pancake' – a joint initiative of the OpenAgri project and the AgStack Foundation – marks a significant development. Pancake is described as an AI-native unified core that standardises authentication, service orchestration, and data semantics across OpenAgri's modular services, functioning, in the developers' own framing, “like the Linux kernel forms a cohesive operating system.” If this infrastructure matures, it would represent the most ambitious attempt yet to create shared, open, pre-competitive digital infrastructure for agriculture at a European and global scale.

4.3.3 The Maturity Gap: Agriculture vs. Automotive

The automotive industry's OSS journey offers a useful benchmark. In that sector, OSS is now “an established part of company strategies” – with major OEMs operating Open Source Program Offices (OSPOs), publicly committing to OSS strategies, and collaborating on shared building blocks through foundations such as Eclipse and the Linux Foundation. This maturity did not emerge overnight; it was built over more than a decade of deliberate investment, supported by government facilitation and driven by competitive pressure.

A direct comparison with the automotive sector illuminates the scale of the gap as well as the nature of the opportunity.

Dimension	Automotive	Agriculture
OSS strategy adoption	Major OEMs have explicit, board-level OSS strategies and published manifestos	No equivalent actors; OSS driven by research projects and civil society
Organised infrastructure	Eclipse SDV Working Group, Automotive Grade Linux, AUTOSAR, COVESA and others	AgStack nascent; no equivalent to Eclipse SDV; OpenAgri/Pancake emerging

OSPO presence	Multiple OEMs and Tier 1 suppliers operate OSPOs	No known OSPOs in agricultural enterprises; concept essentially absent
Funding model	Mix of corporate R&D, VC, and Horizon Europe; long-term industry commitment	Almost entirely dependent on public research funding; high abandonment rate
Regulatory driver	Cyber Resilience Act, functional safety standards pushing OSS engagement	EUDR creating significant OSS tooling demand; Data Act enabling data portability
Cloud-edge architecture	SDV platform debate: centralised vs distributed computing in vehicle	Connectivity constraints make edge/offline-first a practical necessity, not a choice
Lock-in dynamic	OEMs seeking independence from QNX, Android; driving open SDV platforms	Farmers locked into John Deere, AGCO, Trimble ecosystems; limited exit options

Table 1. Comparative maturity of OSS in automotive and agricultural sectors

The most striking difference is the absence of major incumbent actors as drivers of OSS in agriculture. In automotive, it is OEMs – Mercedes-Benz, Porsche, Volvo, Scania – who are actively building OSS capacity and pushing for shared platforms. In agriculture, the major equipment and platform vendors (John Deere, AGCO, CNH Industrial, Trimble) have built proprietary ecosystems and the OSS impetus in agriculture comes almost entirely from outside the dominant commercial actors: from universities, EU-funded consortia, civil society organisations, and international development bodies.

4.3.4 Lock-in and the Sovereignty Challenge

Digital sovereignty – the ability of actors to make independent technical and sourcing decisions aligned with their own values, requirements, and regulatory environment – was identified by every expert interviewed for the automotive paper as a central concern. In agriculture, the sovereignty challenge is, if anything, more acute.

The Precision Agriculture Lock-in Paradox

The transformation of agricultural machinery into data platforms has proceeded rapidly over the past decade. John Deere, the world's largest agricultural equipment manufacturer, exemplifies the model: its JDLink connectivity platform embeds sensors, GPS, and AI-driven decision support into its machines, collecting real-time field data and integrating it into Deere's proprietary ecosystem. The result, as one recent analysis put it, is an 'ownership paradox' – farmers invest millions in equipment they cannot fully repair or control. Switching vendors means abandoning years of accumulated machine learning data, route optimisation records, and agronomic histories that are locked within the platform.

Co-funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

The same pattern is prevalent across the sector. According to a 2026 precision agriculture market analysis, leading players including John Deere, AGCO, CNH Industrial, Trimble, and Topcon are “expanding through integrated hardware-software stacks, OEM partnerships, and open digital platforms that lock in data flows across the farm lifecycle.” A telling symptom: many European farmers are actively seeking out older, pre-digital tractors — simpler, cheaper, and repairable – in preference to sophisticated but inaccessible modern equipment.

The repair rights dimension is not only a consumer complaint. It has significant implications for agricultural resilience: a machine that cannot be repaired at harvest time by a local mechanic, but only by an authorised dealer, represents a systemic vulnerability. The EU's right-to-repair agenda and the automotive industry's experience with proprietary ECUs offer directly relevant precedent.

Data Ownership and the EU Policy Response

The EU has responded to the data ownership challenge on multiple fronts. The EU Data Act, applicable from September 2025, creates binding data access and sharing rights for users of IoT devices – explicitly including agricultural machinery. The Data Act's Chapter II provisions give farmers the right to access data generated by connected equipment, including the right to share that data with third parties. Importantly, Article 43 limits the application of database sui generis rights in the context of machine-generated data, preventing equipment manufacturers from using intellectual property law to restrict access to farm data.[5]

The Data Governance Act, meanwhile, establishes the framework for a Common European Agricultural Data Space – a shared infrastructure for trustworthy pooling and sharing of agricultural data between private and public actors. The October 2025 launch of the EU Partnership Agriculture of Data, a seven-year, €300 million Horizon Europe initiative, represents a significant public commitment to making this infrastructure real.

These regulatory developments create conditions in which OSS tools become both more viable and more valuable. If farm data is legally portable, open source farm management tools can compete on a more level playing field with proprietary platforms. If common data spaces emerge, open source tools that implement the relevant standards will be positioned to bridge them. The policy environment is, for the first time, beginning to create structural incentives for OSS in agriculture.

The Cloud-Edge Question

A theme that emerged clearly in expert consultations is the significance of connectivity constraints for agricultural OSS architecture. Unlike automotive, where the SDV debate concerns how to distribute intelligence between on-vehicle computing and cloud services in an environment of assumed connectivity, agriculture frequently operates in conditions of intermittent or absent connectivity. Fields, orchards, and remote grazing areas may have no reliable network access. Decisions about irrigation, pest response, or livestock management often cannot wait for cloud round-trips.

This makes the cloud-edge architecture question in agriculture not a design choice but a practical constraint. Edge computing – processing at or near the data source – is not just an optimisation but a necessity. Integrating sensor networks with edge nodes in agricultural environments can significantly enhance real-time data processing while reducing

[5] *https://www.cema-agri.org/images/publications/position-papers/CEMA_Data_Act_QA-2025-04.pdf*

communication burden on cloud platforms. Open source platforms designed for edge deployment (including LoRaWAN-based sensor networks, containerised edge inference, and offline-first mobile applications) are therefore structurally important, not merely convenient. An open, standards-based architecture for agricultural intelligence that operates coherently across device, edge, and cloud layers would represent a significant contribution to the digital sovereignty of European farming. The automotive analogy here is the SDV platform: a shared, open infrastructure layer that enables interoperability without imposing a single vendor's control. Agriculture's equivalent does not yet exist in coherent form; Pancake (the OpenAgri/AgStack initiative) is perhaps the most serious current attempt to build it.

4.3.5 Capacity, Culture, and the Ecosystem Challenge

One of the automotive paper's most important findings was that the automotive industry's "historical hardware-centric focus sometimes acts as a barrier to embracing OSS"' The same pattern, in a more extreme form, characterises agriculture. The difference is that in automotive, there is a growing number of executives and engineers who understand software and are driving the transition from within. In agriculture, that group is much smaller, more fragmented, and largely external to the dominant commercial actors.

The Stakeholder Fragmentation Problem

European agriculture comprises around 9 million farms, the vast majority of them small or medium-scale family operations. Digital readiness varies enormously.[6] A small percentage of large, commercial farms – particularly in France, the Netherlands, and Eastern Europe – are described by consultees as resourceful and technically capable. The majority, however, have limited resources, limited digital skills, and a cultural orientation toward the practice of farming rather than the management of technology platforms.

This fragmentation makes it extremely difficult to build the kind of coherent OSS ecosystem that has emerged in automotive. There is no agriculture equivalent of Mercedes-Benz or Porsche – no large actor with the resources, the incentive, and the engineering capacity to take a leadership position in open source and pull the rest of the sector forward. Tier 1 and Tier 2 suppliers in automotive play a significant role in driving OSS adoption upward through supply chains; in agriculture, the supply chain dynamics work in the opposite direction, with large platform vendors driving proprietary standards downward.

The European OSS landscape in agriculture is therefore dominated by a different set of actors: universities and research institutes (often through EU-funded projects), international development organisations (FAO, WRI, GIZ), civil society and standards bodies, and a small number of mission-driven SMEs and cooperatives. These actors have demonstrated that OSS works in agricultural contexts. What they have not yet demonstrated is that it can be sustained without continuous public funding.

The Sustainability Problem

The single most consistent theme in expert consultations for this paper was the sustainability of OSS outputs after project funding ends. The EU has funded dozens of Horizon projects that include OSS components – tools for farm management, data collection, decision support, supply chain traceability – but the track record of these tools surviving the end of their funding

[6] *https://publications.jrc.ec.europa.eu/repository/handle/JRC141259*

cycle is poor. When a three-year project closes, the developers often move on, the repositories are no longer maintained, and the tools gradually become unusable.

This is not a problem unique to agriculture. The automotive paper identified OSS supply chain sustainability as a sector-wide challenge, noting that “pooling resources through common efforts can enhance the sustainability of OSS projects.” But in automotive, there is at least a growing recognition of the problem and emerging mechanisms – OSS foundations, corporate contribution mandates, SBOMs – to address it. In agriculture, these mechanisms are largely absent.

The AgStack Foundation represents the most serious current attempt to provide a sustainable home for agricultural OSS. Positioned under the Linux Foundation, it offers proven governance processes and a neutral space for pre-competitive collaboration. The December 2025 OpenAgri/AgStack collaboration and the Pancake initiative are significant precisely because they attempt to solve the sustainability problem at a structural level – embedding EU-funded project outputs into a foundation that will exist beyond the project's life. This is the right model; the challenge is scaling it.

Skills and Capabilities

The automotive paper identified skills as a key lever for OSS adoption, noting that OSS engagement both attracts engineering talent and serves as a mechanism for up-skilling existing staff. In agriculture, the skills challenge is more fundamental. The question is not only whether agricultural technology developers have the skills to engage with OSS – many do – but whether farmers, farm advisors, and regional administrators have the skills to use, evaluate, and contribute to OSS tools.

Several EU-funded projects have taken deliberate approaches to this challenge. OpenAgri focuses explicitly on tools that work in remote areas with limited connectivity and limited technical capacity, with co-creation approaches that centre farmer experience. Farmtopia emphasises reusable modules and scalable infrastructure precisely to reduce the per-deployment technical overhead. FarmOS's Field Kit provides offline data entry for environments where neither connectivity nor device sophistication can be assumed.

The cloud-edge computing architecture is directly relevant here: tools that process data locally, at the edge, reduce the dependence on cloud infrastructure and the connectivity and technical literacy that implies. An open source edge computing platform that works reliably on relatively simple hardware, in low-connectivity environments, with farmer-facing interfaces that do not require technical expertise, would represent a transformative capability for the majority of European farms.

4.3.6 Regulation as an OSS Driver: The EUDR Case Study

One of the most instructive recent developments in agricultural OSS is the way in which the EU Deforestation Regulation has functioned as an inadvertent OSS driver. The regulation, introduced in June 2023 with full enforcement from December 2026, requires operators placing seven key commodities (soy, palm oil, wood, cocoa, coffee, rubber, and cattle) on the EU market to demonstrate that they are deforestation-free, legally produced, and traceable to the plot of land where they were grown.

The technical requirements are demanding: plot-level geolocation, historical land-use verification, supply chain documentation, and submission of a Due Diligence Statement (DDS) to the EU TRACES portal. For companies with complex, multi-tier supply chains involving thousands of smallholder producers, this creates a significant compliance challenge – and a market for tools that can address it at scale.

The Open Source Response to EUDR

The commercial response to EUDR has been dominated by proprietary compliance platforms (Sourcemap, osapiens, Nadar, BanQu, Coolset and others), several of which offer end-to-end traceability and DDS automation. But a parallel ecosystem of open source and publicly funded tools has also emerged, with distinct characteristics: they are designed for accessibility to resource-constrained actors (including smallholders and public institutions), they prioritise interoperability and open data standards, and they are built on publicly governed infrastructure.

Initiative	Type	Key Focus	OSS Status
WHISP (FAO)	Open Source	Plot-level deforestation risk assessment; cross-validates multiple Earth observation datasets	Fully open source; hosted by FAO
AIM4Commodities	Public Initiative	FAO-led programme for open, inclusive monitoring; field data collection for smallholders	Open Foris suite; OSS components
INATrace	Open Source	Blockchain-based farm-to-consumer traceability for commodity supply chains	Fully open source; integrating with AgStack
TerraTrac / FAO Ground	Open Source	Mobile field data collection for plot geolocation	Open source; offline-capable
KoboCollect / QField	Open Source	General-purpose field data collection tools applicable to EUDR geolocation requirements	Fully open source
GeoID Standard	Open Standard	Anonymous, consistent identifiers for plot polygons; enables cross-system interoperability	Open standard; foundation-governed
Forest Data Partnership	Open Infrastructure	WRI/FAO-led shared data ecosystem for land use; EUDR-relevant datasets and tools	Open data and open source components

Table 2. Key open source and publicly governed tools for EUDR compliance

The EUDR case illustrates a mechanism that has broader applicability: regulation that creates compliance requirements for which no adequate proprietary solution exists – or for which proprietary solutions are unaffordable for the majority of affected actors – creates a structural case for open source. When smallholder farmers cannot afford proprietary EUDR compliance platforms, open source tools that can be deployed at low cost and governed by international public bodies become essential infrastructure.

The same logic applies to the Ecodesign for Sustainable Products Regulation and other regulatory instruments that are extending supply chain transparency requirements. Each of these creates demand for interoperable, accessible, standards-based traceability tools, such as the Digital Product Passport – and each represents an opportunity for open source.

The Smallholder Access Problem

A recurring concern in the EUDR context is that plot-level geolocation requirements, if implemented through expensive proprietary platforms, could function as a de facto barrier to market access for smallholder producers. If only large, well-resourced operations can afford compliance, the regulation could accelerate the consolidation of supply chains around large producers which is the opposite of its intent.

Open source tools address this concern directly. WHISP is designed to be usable by smallholders via mobile device, with no geospatial expertise required. FAO Ground and TerraTrac support offline operation in low-connectivity environments. These are not merely technical features; they are expressions of a policy position about who digital infrastructure should serve. The open source model, in this context, is not just economically advantageous but can be an instrument of agricultural equity.

4.3.7 Pathways for OSS in Agriculture: Key Themes

Synthesising the findings above, five themes emerge as central to the development of a sustainable, impactful OSS ecosystem in European agriculture.

Commodity vs. Differentiating Technology

The automotive paper identifies the distinction between commodity (non-differentiating) and differentiating technology as central to the case for OSS collaboration. Companies can collaborate on commodity technology – shared infrastructure, standard interfaces, common platforms – while competing on the differentiating applications built on top. This logic applies directly to agriculture.

In agriculture, the commodity layer includes: farm data collection and management infrastructure; geospatial monitoring and Earth observation integration; supply chain traceability standards and protocols; sensor firmware and edge computing platforms; and interoperability standards for agricultural data exchange. None of these represent the competitive advantage of any agricultural enterprise. They are the pipes and plumbing of the digital farm – essential, costly to build independently, and valuable only when shared.

The differentiating layer, by contrast, includes: specific agronomic decision models tuned to particular crops, soils, and climates; proprietary machine learning trained on proprietary farm data; branded advisory services; and specialised hardware designs. This is where competitive advantage can legitimately reside, and where proprietary development makes sense.

The challenge is that the agricultural sector has not yet made this distinction clearly. EU-funded research projects frequently develop both layers simultaneously, without a strategy for releasing the commodity components as sustainable OSS while protecting or commercialising the differentiating components. A clearer taxonomy – supported by funding requirements and governance frameworks – would help.

Foundation-Based Governance as the Key Mechanism

The automotive paper identifies OSS foundations as critical enabling structures – providing neutral governance, managing shared intellectual property, facilitating pre-competitive collaboration, and ensuring sustainability. In automotive, the Eclipse Foundation, the Linux Foundation, and others play this role. In agriculture, AgStack is the most direct equivalent, but it remains small relative to the challenge.

The OpenAgri/AgStack Pancake initiative is significant because it represents a serious attempt to apply the foundation model to EU-funded agricultural research outputs. If successful, it would create a template: Horizon Europe projects develop open source components; those components are released into a governed foundation; the foundation maintains and sustains them beyond the project cycle; future projects build on rather than duplicate existing work. This is the model that works in automotive. There is no fundamental reason it cannot work in agriculture.

For this to happen at scale, EU research funding mechanisms need to mandate – not merely encourage – the transfer of OSS outputs to sustainable foundations. This is a policy change, not a technical one.

Standards as Enablers

Open standards and OSS are complementary but distinct. Open standards define the interfaces across which different systems interoperate; OSS provides implementations of those standards that can be freely used, studied, modified, and distributed. In agriculture, both are underdeveloped, and their absence compounds each other.

The EU has recognised this: Horizon calls such as HORIZON-CL4-2025-03-DATA-11 explicitly encourage comparative development of edge, cloud, and hybrid OSS solutions, decision-support tools, open APIs, and adherence to data interoperability frameworks. The emerging GeoID standard for plot polygon identification, the Data Act's portability provisions, and the Common European Agricultural Data Space initiative all represent moves toward the standards infrastructure that OSS needs to thrive.

Standardisation bodies including CEN-CENELEC have a role to play, as do foundations like FIWARE, which has been applied in smart farming contexts and provides open APIs and data models for IoT-intensive environments. The key principle, borrowed from the automotive paper, is that standards promoted should be implementable in OSS.

Government as Enabler and Convener

In the automotive paper, interviewees from across the industry emphasised the role of government as a neutral convener and facilitator – bringing competing actors together in a space where they can collaborate on pre-competitive technology without raising competition law concerns, and providing funding that de-risks the early stages of shared investment. The European Commission's internal forum for OEMs and Tier 1 suppliers on R&I and standardisation is cited as an example of this facilitation role.

In agriculture, government has an even more direct role to play, because the dominant commercial actors are not yet inclined to drive OSS development. Public research funding (Horizon Europe, national programmes) is currently the primary mechanism for OSS development in agriculture. The challenge is to make that mechanism more effective: by mandating sustainability planning in funded projects, by routing outputs through foundations, by using public procurement to create demand for OSS-compatible tools, and by developing the regulatory frameworks (Data Act, EUDR, future instruments) in ways that create structural incentives for open, interoperable solutions.

4.3.8 Recommendations

The following recommendations are addressed to two audiences: agricultural industry actors (including agribusinesses, cooperatives, technology developers, and research organisations) and policymakers at EU and national levels.

Recommendations - For Agricultural Industry and Research Actors

Adopt and communicate OSS strategies

Agricultural technology organisations – whether agribusinesses, cooperatives, or research consortia – should develop explicit OSS strategies that distinguish commodity technology (to be developed collaboratively and released as OSS) from differentiating technology (where proprietary development may be appropriate). Even a simple, publicly communicated commitment to OSS for non-differentiating infrastructure would begin to shift norms in the sector.

Build OSPO capacity

Research consortia coordinating EU-funded agricultural projects, university technology transfer offices with agricultural portfolios, and agricultural foundations should establish OSPO functions to manage OSS outputs, support compliance, and build open source culture. The TODO Group and OSPO Alliance provide resources and community for organisations beginning this journey.

Engage with and support agricultural OSS foundations

Organisations developing agricultural software should actively evaluate whether their outputs can be hosted by AgStack or equivalent foundations. Contributing to existing OSS projects such as FarmOS, WHISP, INATrace, Open Foris, is preferable to creating new, competing tools. Where new tools are created, sustainability planning (including foundation hosting) should be a project requirement from day one.

Design for the edge

Given the connectivity constraints of agricultural environments, OSS tools for agriculture should be designed with offline-first or edge-first architectures. This includes offline-capable mobile applications, containerised edge inference that can run on commodity hardware, and synchronisation protocols that handle intermittent connectivity gracefully. The emerging cognitive cloud-edge computing frameworks are directly relevant here.

Monitor EUDR as a template

The EUDR case demonstrates that regulation can drive OSS development at scale. Agricultural technology organisations should monitor and engage with emerging regulatory requirements and assess where open, interoperable OSS tools could address compliance needs more equitably than proprietary alternatives.

Recommendations - For Policymakers at EU and National Levels

Require OSS sustainability in Horizon funding

Horizon Europe projects developing software should be required to include a sustainability plan for OSS outputs, including a credible pathway to foundation hosting or other governance mechanisms that ensure maintenance beyond the project cycle. The current norm where OSS outputs are deposited in a repository and not maintained is not an optimal use of public investment and can also serve to undermine confidence in OSS as a viable model.

Use procurement as a demand-creation mechanism

Public procurement of agricultural digital tools — including systems used by national agricultural paying agencies, veterinary authorities, and environmental monitoring bodies — should prioritise open source and open standards-compliant solutions. This creates sustainable demand that does not depend on research funding, and signals to the market that OSS is a viable competitive option.

Support agricultural OSS foundations

Direct funding for agricultural OSS foundations (including AgStack and equivalents) should be considered as part of the Digital Europe Programme and future framework programmes. Foundation infrastructure – governance, legal, security auditing, community management – is expensive and cannot be fully covered by project grants. Public co-investment in foundation infrastructure is justified by the public goods character of the resulting shared infrastructure.

Align the Data Act with OSS

The Data Act's data portability provisions should be implemented in ways that actively support open source. This means ensuring that the data formats and APIs required for portability are openly specified and implementable without proprietary dependency, and that the Common European Agricultural Data Space is built on open standards with open source reference implementations.

Develop regulatory impact assessments for OSS

Before implementing new digital reporting or traceability requirements in agriculture (as in EUDR), impact assessments should evaluate the availability and accessibility of OSS compliance tools. Where proprietary tools dominate a compliance space, targeted public investment in open alternatives should be considered, both for equity reasons (smallholder access) and for digital sovereignty reasons (avoiding structural dependence on non-European compliance infrastructure).

Invest in skills

A targeted programme for OSS skills development in agriculture, covering farmers, farm advisors, regional administrators, and the developers of agricultural tools, would address one of the most persistent barriers to adoption. This should be integrated into existing rural development and digital skills programmes, and should include practical engagement with existing OSS tools rather than abstract instruction.

4.3.9 Conclusion

The automotive industry's experience with OSS offers an instructive but imperfect analogy for agriculture. The structural challenges are similar – fragmented supply chains, long asset lifecycles, hardware-centric culture, safety-critical use cases – but the actor landscape is

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

different, the resources available are more constrained, and the policy context is, in some respects, more favourable. The EU's regulatory agenda (EUDR, Data Act, Common Agricultural Data Space) is creating conditions in which OSS becomes not just convenient but structurally necessary.

What agriculture has in common with automotive is the fundamental logic of OSS as a response to complexity that no single actor can manage alone. No farm, cooperative, or agribusiness can independently build and maintain the full stack of digital tools that modern sustainable farming requires. No EU member state can independently develop and govern the data infrastructure that the Common Agricultural Policy increasingly demands. The only viable model for infrastructure that is non-differentiating, safety-relevant, and required at scale is collaborative development under open governance.

The emerging ecosystem – AgStack, OpenAgri, Pancake, WHISP, FarmOS, INATrace and others – demonstrates that this is possible. The challenge is to move from a collection of promising initiatives to a coherent, sustainable infrastructure: governed by foundations, mandated by funders, preferred by procurement, and designed for the edge environments where most of European agriculture operates.

This will not happen at the pace of a three-year research project. It requires a sustained commitment from policymakers, a strategic shift among the research and innovation community, and eventually engagement from the commercial actors who currently profit from proprietary lock-in. The automotive sector's journey suggests that this shift, once it begins, can move faster than expected.

5. Final EU research & policy alignment recommendations for the EU Cognitive Computing Continuum

5.1 Summary of the policy recommendations development process

The process followed by the NexusForum.EU project to identify policy recommendations is a structured, multi-pillar framework designed to enhance EU Digital Sovereignty within the Cognitive Computing Continuum.

The overall strategy to enhance EU Digital Sovereignty is built upon the following three interlinked pillars:

a) Continuous monitoring and analysis of the **European regulatory landscape** and **policy initiatives** related to the Cognitive Computing Continuum.

b) **Public Consultation** and **Participatory Actions**: this pillar focuses on increasing the awareness and meaningful participation of EU stakeholders in policy initiatives, particularly those led by the European Commission. This includes a combination of activities such as public consultations, participatory actions and co-creative collaborative engagement activities.

c) **International Comparative Analysis**: the project employs comparative approaches to policy analysis, with a specific focus on the international situation in Japan and the Republic of Korea, to align strategies and extract lessons learned at both the technology prospection and policy levels.

The methodological framework used to identify policy recommendations is a dynamic process grounded in stakeholder engagement and a multi-dimensional analysis of the European Cognitive Computing Continuum. It consists of the following steps:

The **first step, Framework setting**, entails defining an analytical framework based on six critical factors considered to influence the EU's technological sovereignty and the convergence of Edge, Cloud, and IoT technologies. These six factors are directly linked to the project's Work Packages (WPs) and specific tasks to ensure that final policy recommendations are based on technical evidence and research outcomes. These six factors serve as dimensions for the SWOT analyses of the European Cognitive Computing Continuum, and are as follows:

- **F1**: Technology, innovation and research capabilities. This factor focuses on identifying gaps between research challenges and technological capabilities. It is informed by WP2, specifically analysing prioritised research lines, technological capacities, future research lines, and synergies with industrial actors in R&D&i.
- **F2**: Framework conditions (policies, strategies, plans, regulations, etc.). This dimension analyses the current regulatory landscape, including the AI Act, Data Act, CRA, DMA and DSA. It involves monitoring the European regulatory landscape and evaluating certification schemes like EUCS+ and the Cloud Rulebook.
- **F3**: Enabling conditions (Open Source, open standards, skills and ethics). This factor explores the role of Open Source Software and open standards as enablers for

interoperability and vendor neutrality. It analyses workforce training needs for both new and older generations and assesses ethical and social impacts.

- **F4**. Infrastructures and connectivity (including space infrastructure and data). This factor focuses on the physical and digital foundations required for the Continuum.
- **F5**. Collaboration & engagement between initiatives at EU and international level. This dimension has to do with ensuring the active participation of EU companies involved in IPCEI-CIS and the European Alliance for Industrial Data, Edge and Cloud, as well as strategic alignment with international partners, specifically Japan and South Korea.
- **F6**. Industry participation. This factor aims to bridge the gap between NexusForum.EU and the industry, with a special focus on European SMEs as key players.

The **second step**, known as **Implementation**, aimed to identify needs and gaps within the European Cognitive Computing Continuum to eventually derive policy recommendations. The key components of this step were as follows:

1. Data inputs and integration: inputs were integrated from project work streams using findings derived from the project's work packages, and information was also collected through online workshops held with task leaders and relevant partners.

2. SWOT diagnoses and Gap identification: this was the core technical activity of this step and consisted of carrying out six SWOT analyses conducted across the six assessment factors described in the previous step. These diagnoses were performed by comparing the current state of play of the European Cognitive Computing Continuum against an ideal state to pinpoint specific gaps. These analyses were structured around the two perspectives of a SWOT:

3. Internal perspective, used to identify strengths to be reinforced and weaknesses to be overcome.

4. External perspective, used to identify opportunities to be exploited and threats to be mitigated.

5. The analyses identified a set of gaps for each respective assessment factor. These gaps were consolidated into a list of 14 critical gaps after merging the outcomes of the six individual SWOT analyses into a single, consolidated SWOT. This merged assessment was further refined by incorporating international reports (reports on Japan and South Korea) and key secondary sources (Mario Draghi and Enrico Letta reports).

The third and **final step** involved defining and refining the **policy recommendations**.

To ensure the recommendations were grounded in real-world needs and technical urgency, the identified gaps underwent a verification and prioritisation process through a survey.

The gaps were also discussed, contrasted and validated through structured discussions within the NexusForum.EU working groups. These groups, co-led by researchers and industry representatives, ensured that the gaps aligned with actual research and innovation roadmaps.

Once gaps were verified and prioritised, they were mapped to specific Policy Recommendations and Implementation Ideas:

- Each Policy Recommendation was designed to address multiple interrelated gaps simultaneously.
- For every Policy Recommendation, concrete technical implementation steps were defined.

Finally, Policy Recommendations were assessed and validated through a workshop with the participation of the project's working groups.

5.1.1 Gaps from the SWOT analysis

As part of the earlier phases of the NexusForum.EU project, a comprehensive SWOT-based assessment of the European Cognitive Computing Continuum was carried out, supported by interviews with project partners and relevant ecosystem stakeholders. This process generated robust evidence base on the main structural weaknesses, barriers and strategic dependencies affecting the development of a competitive, trusted and federated European continuum infrastructure.

Based on this analysis, 14 critical gaps were identified as key obstacles to the consolidation of the European Cognitive Computing Continuum and to the strengthening of European digital sovereignty. These gaps span technological, infrastructural, regulatory, market and investment dimensions, and together highlight the need for a more coherent and coordinated European response.

To support the subsequent validation phase, the identified gaps were consolidated into a structured set of statements that could be easily presented to external stakeholders and assessed through the survey process. This approach made it possible to contrast the findings of the SWOT analysis with external perceptions, facilitate prioritisation, and gather targeted feedback on the most relevant barriers affecting the European ecosystem.

Table 3 presents the 14 gaps identified through the SWOT analysis and partner consultation process.

No.	Gap	Description
1	Technological Sovereignty Challenges	Slow adoption of advanced technologies, limited trust in AI and data security, and dependence on non-EU solutions undermine the EU's technological autonomy
2	Fragmented Infrastructure Ecosystem	Disconnected edge, cloud, and IoT resources hinder the creation of a trusted, federated computing continuum across Europe
3	Regulatory Complexity for SMEs	Fragmented and burdensome regulations, lack of harmonization, and high compliance costs limit the growth and innovation capacity of SMEs and startups
4	Low Confidence in EU Cloud Providers	Limited trust in EU-based cloud solutions contributes to scepticism about Europe's ability to compete with global hyperscalers.
5	Barriers to Cross-Border Data Sharing	Legal, technical, and organizational obstacles to accessing and sharing data across borders restrict the development of Common European Data Spaces and data-driven innovation.

6	Weak Open source Ecosystem	Limited resources and skills in open source software, coupled with low engagement from large enterprises, slow down innovation and adoption
7	SME Dependence on Non-EU Hyperscalers	Heavy reliance on foreign cloud providers and fragmented European infrastructure reduce digital sovereignty and competitiveness
8	Infrastructure Fragmentation and Energy Costs	Disjointed HPC, digital, and networking infrastructures, high energy costs, and lack of a unified strategy for 5G/6G and fibre deployment weaken Europe's competitiveness
9	Lack of Quantum-HPC Integration Strategy	The absence of a clear roadmap for integrating quantum computing with HPC threatens Europe's leadership in hybrid computing models
10	Ineffective Coordination of Strategic Initiatives	Overlapping goals, unclear business objectives, and weak SME engagement in initiatives like Gaia-X, IDSA, and IPCEI reduce their overall impact
11	Limited SME Participation in Global Ecosystems	Dependence on non-EU platforms and low involvement in international digital ecosystems weaken Europe's global positioning
12	Funding Gaps and SME Vulnerability	Short-term financial pressures and limited access to growth capital prevent SMEs from scaling and building resilience
13	Vendor Lock-In Risks	High dependence on specific technology vendors (in many cases non-European) increases the vulnerability of European SMEs and reduces strategic flexibility
14	Semiconductor Supply Chain Weaknesses	Reliance on non-EU semiconductor suppliers and underdeveloped capital markets hinder SME competitiveness in advanced technologies

Table 3. 14 gaps identified through the SWOT analysis

5.1.2 First draft of policy recommendations

Building on the SWOT analysis and the 14 critical gaps identified in the previous section, this subsection presents a first, synthetic set of strategic policy actions for the European Cognitive Computing Continuum. The aim is to translate the analytical findings into an initial set of policy directions that can support a sovereign, competitive and trusted European continuum, while reinforcing ongoing EU initiatives such as IPCEI-CIS, EUCloudEdgeIoT and the Common European Data Spaces.

Co-funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

The recommendations are organised around seven Policy Actions. For each Policy Action, the table below summarises the main objective, the gaps addressed and the key implementation levers to be activated. At this stage, the implementation levers are indicative and expressed at a high level (e.g. types of instruments or mechanisms), rather than as fully developed policy measures.

The draft recommendations presented below are therefore not meant to be exhaustive, but rather to provide a structured starting point for discussion, validation and prioritisation with stakeholders. Their role is to support the transition from analytical findings to policy-oriented solutions that can strengthen the European Cognitive Computing Continuum across its technological, regulatory and industrial dimensions.

No.	Policy Action	Main Objective	Addressed GAPs	Main implementation levers
1	**Unifying the Fragmented Infrastructure and Integrating Future Technologies**	Build a federated, energy-efficient continuum connecting cloud, edge, IoT, HPC and emerging quantum resources.	2, 8, 9	Continuum-ready-by-design principles; Continuum-ready certification and shared testbeds; Hybrid quantum–HPC roadmap; Green connectivity and energy-efficient infrastructure funding
2	**Strengthening Trust and Cross-Border Data Fluidity**	Establish European cloud-edge-data solutions as the global benchmark for trust.	1, 4, 5	Enforceable right to switch and data portability; Multi-provider procurement and deployment strategies; Open multi-cloud and multi-edge reference architectures; Semiconductor and edge-AI resilience measures
3	**Reducing Vendor Lock-In and Strengthening Strategic Autonomy**	Reduce dependence on (non-EU) specific vendors and reinforce Europe's hardware and service base.	7, 13, 14	Enforceable right to switch and data portability; Multi-provider procurement and deployment strategies; Open multi-cloud and multi-edge reference architectures; Semiconductor and edge-AI resilience measures
4	**Consolidating Governance and Coordination for the Continuum**	Improve strategic alignment, coordination and stakeholder participation.	10, 7, 11	European continuum coordination board; Alignment of IPCEI-CIS, Gaia-X, IDSA, AIOTI and related initiatives; Structured SME and user-sector participation mechanisms

5	**Strengthening the Open Source and Standards Commons**	Reinforce Europe's shared open source and standards base for the continuum.	6, 1, 10	Sovereign open source and standards facility; Open-by-default rules for publicly funded research outputs; Incentives for industry participation in the open commons; Skills and capacity-building for open source
6	**Supporting SMEs to Scale and Compete Globally**	Remove barriers that prevent SMEs from scaling and participating in global ecosystems.	3, 11, 12, 7	Continuum-focused regulatory sandboxes; Scaled-up finance for cognitive technologies; "AI-ready SME" certification scheme; Continuum SME hub and support services
7	**Enhancing Technological Sovereignty and Adoption Capacity**	Strengthen Europe's capacity to develop, deploy and govern advanced continuum technologies.	1, 4, 6	Skills and capability-building programmes; Flagship deployments in key sectors; Responsible AI and trust frameworks for continuum deployments

Table 4. Overview of the proposed Policy Actions (draft version)

An updated version of Policy Actions (renamed as Policy Recommendations) is detailed in the final section of this chapter. That version will integrate the survey results on the gaps, the international perspective, and the feedback collected through the NexusForum.EU working groups, and will provide a more detailed description of the proposed measures and delivery mechanisms.

5.2 Feedback from stakeholders

5.2.1 Validation and prioritisation of Gaps from the survey

To complement the analytical work carried out in the previous phases of the project, NexusForum.EU conducted a targeted stakeholder survey to validate and prioritise the gaps identified through the SWOT analysis. The consultation aimed to assess the perceived relevance of each gap and to collect qualitative input that could inform the subsequent development of policy recommendations for the European Cognitive Computing Continuum.

Survey methodology

The survey was designed as a targeted consultation addressed to external experts and project partners. It was implemented using **EUSurvey**, the European Commission's official multilingual online tool for creating and managing surveys and consultations, which supports questionnaire design, response collection and result analysis.

Co-funded by the European Union
Project funded by Schweizerische Eidgenossenschaft, Confédération suisse, Confederazione Svizzera, Confederaziun svizra, Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

The consultation was disseminated at different moments in order to reach a relevant and diverse group of stakeholders. The largest share of responses was collected during a NexusForum.EU event held in Brussels at the end of 2025. The survey was subsequently re-circulated during an online workshop held in May 2026 with participants from the project's working groups. This two-stage approach made it possible to gather feedback both from external actors and from stakeholders actively engaged in the thematic discussions of the project.

The survey was presented as part of the project's work on policy recommendations aimed at strengthening European sovereignty in the Cognitive Computing Continuum. Participants were informed that earlier analytical work had identified a set of key gaps affecting the development of the European continuum across several dimensions, including technological and research capabilities, regulation and policy, enabling conditions, infrastructure and connectivity, collaboration among key actors, and industry participation.

Respondents were invited to assess each gap according to two criteria: **potential impact** and **urgency**. For each gap, participants were asked to assign one of three priority levels and were also given the opportunity to provide comments, suggestions or additional considerations. This made it possible to combine structured prioritisation with qualitative feedback from respondents, in line with the general principles of stakeholder consultation used in EU policy preparation.

To support a common interpretation of the prioritisation exercise, the survey provided a simple three-level framework:

- **High Priority (Critical Gaps):** gaps requiring immediate action or having a transversal impact on the Computing Continuum, particularly where they show very high strategic relevance, high political urgency, or direct alignment with European Commission priorities such as AI, energy efficiency, IoT-edge-cloud-HPC integration and semiconductors.
- **Medium Priority (Enabling Gaps):** gaps that support progress in critical areas but have a more indirect or medium-term effect, notably where they strengthen implementation capacity and contribute to the consolidation of the continuum strategy.
- **Long-term Priority (Contextual Gaps):** gaps relevant for long-term sustainability and competitiveness, whose resolution is likely to be most effective once more critical gaps have been addressed first.

This consultation process served a dual purpose. First, it enabled the external validation of the gaps identified during the analytical phase of the project. Second, it provided an evidence-based basis for their prioritisation and for the refinement of the policy recommendations presented in the following sections.

Results of the Validation and prioritisation of gaps

The survey results confirm the relevance of the gaps identified in the SWOT analysis and provide a clearer basis for their prioritisation. Based on 47 responses, the exercise shows a strong concentration of concern around a limited set of structural weaknesses, while also distinguishing a second group of enabling and longer-term issues.

Six gaps emerged as the most urgent priorities for action: **Technological Sovereignty Challenges** (68% high priority), **Vendor Lock-In Risks** (66%), **SME Dependence on Non-**

EU Hyperscalers (64%), **Regulatory Complexity for SMEs** (60%), **Funding Gaps and SME Vulnerability** (55%), and **Low Confidence in EU Cloud Providers** (53%). These results indicate that respondents see Europe's most pressing challenges not only in technological terms, but also in relation to structural dependence on non-EU providers, barriers affecting SME growth, and limited trust in the competitiveness and accessibility of European alternatives.

A second tier of gaps was assessed as important, but less immediate. This includes **Semiconductor Supply Chain Weaknesses** (45% high priority), **Fragmented Infrastructure Ecosystem** (43%), and **Ineffective Coordination of Strategic Initiatives** (40%). These issues are recognised as strategically significant, but respondents appear to view them as more dependent on broader structural reforms, governance improvements or longer implementation cycles.

Other gaps were more frequently positioned as enabling or longer-term issues than as immediate priorities. This is the case for **Barriers to Cross-Border Data Sharing** (34% high priority), **Weak Open Source Ecosystem** (38%), **Infrastructure Fragmentation and Energy Costs** (36%), and **Limited SME Participation in Global Ecosystems** (30%). **Lack of Quantum-HPC Integration Strategy** was clearly identified as a longer-term issue, with only 4% of respondents classifying it as high priority, while most placed it in the medium-term horizon.

The **qualitative feedback** helps to explain these patterns of prioritisation. In particular, respondents consistently frame technological sovereignty as a strategic vulnerability, regulatory fragmentation as a direct barrier to SME innovation and scale-up, and low confidence in EU cloud providers as largely a question of market positioning, scale and visibility rather than purely technical capability. The responses also suggest that some gaps are perceived as upstream drivers of others.

In this respect, **Technological Sovereignty Challenges**, **Regulatory Complexity for SMEs** and **Vendor Lock-In Risks** emerge as structurally central gaps, since they influence several downstream problems, including SME dependence on non-EU hyperscalers, low confidence in EU cloud providers, barriers to cross-border data sharing and limited SME participation in global ecosystems.

Category	Gap	High-priority share	Comment
Very strong consensus	Gap 1: Technological Sovereignty	68%	Existential threat perceived as more urgent than all others
Very strong consensus	Gap 13: Vendor Lock-In	66%	Systemic vulnerability perpetuating dependence
Very strong consensus	Gap 7: SME Hyperscaler Dependence	64%	Crisis of dependence in non-EU ecosystems

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

Very strong consensus	Gap 3: Regulatory Complexity	60%	Major blocker for SME innovation and scale-up
Very strong consensus	Gap 12: Funding Gaps	55%	Important enabler for sovereignty-oriented initiatives
Moderately critical	Gap 4: Low EU Cloud Confidence	53%	Market uptake and positioning problem in EU providers
Moderately critical	Gap 14: Semiconductors	45%	Recognised strategic issue with longer time horizons
Moderately critical	Gap 2: Infrastructure Fragmentation	43%	Important, but perceived as less urgent than regulation
Moderately critical	Gap 10: Initiative Coordination	40%	Clear need, though not seen as the most immediate blocker
Enablement / long-term	Gap 6: Weak Open Source Ecosystem	38%	Relevant, but expected to strengthen once root gaps are addressed
Enablement / long-term	Gap 8: Energy / Infrastructure Costs	36%	Secondary compared with regulatory and dependency-related issues
Enablement / long-term	Gap 5: Cross-Border Data Sharing	34%	Important enabler, but not perceived as a primary blocker
Enablement / long-term	Gap 11: SME Global Participation	30%	Largely viewed as a consequence of more structural constraints
Enablement / long-term	Gap 9: Quantum-HPC Integration	4%	Clearly positioned as a future-oriented issue rather than an immediate priority

Table 5. Prioritisation of gaps based on survey responses

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

Main findings and implications

Three main findings emerge from the validation exercise. **First**, the survey confirms that the most urgent challenges are those linked to sovereignty, interoperability, market dependence and the framework conditions for SMEs. **Second**, respondents distinguish clearly between immediate structural blockers and issues that are important but more medium- to long-term in nature, such as quantum-HPC integration or some infrastructure-related challenges. **Third**, the results point to a causal structure in which a limited number of root problems generate several secondary constraints across the wider ecosystem.

From a policy perspective, this implies that prioritisation should not be based only on the individual weight of each gap, but also on its systemic effect across the continuum. The survey therefore supports giving priority to those gaps whose resolution would have the broadest enabling effect, notably technological sovereignty, regulatory simplification and the reduction of vendor lock-in, while addressing other gaps in a sequenced manner according to their strategic urgency and dependency on upstream reforms.

5.2.2 Assessment and prioritisation of policy recommendations by the working groups of the NexusForum.EU project

The assessment and prioritisation of policy recommendations were conducted through a dedicated workshop involving the NexusForum.EU Working Groups. The objective was to validate a first draft of policy recommendations designed to address identified gaps in the development of the European Cognitive Computing Continuum.

The suggestions put forward by participants for improving the policy recommendations were as follows:

1. Open Source and Sovereignty (policy recommendations 5&7)
2. Participants suggested the creation of a dedicated European Agency for Open Source.
3. Certification: this agency should offer certification for the code of Long-Term Support (LTS) versions to help build trust in open source solutions.
4. A specific gap was identified regarding the lack of a permissive EU license for open source, similar to the Apache or MIT licenses.
5. SME Support and Scaling (policy recommendation 6)
6. Feedback indicated that EU funding application processes are too burdensome for SMEs, often exceeding 100 pages and having success rates as low as 2-3%.
7. Suggestions included simplifying applications to 20-30 pages and providing smaller, more accessible awards rather than only millions.
8. Participants noted that legislations like the AI Act and Data Act place disproportionately heavy compliance burdens on SMEs.
9. Market Access: it was noted that SMEs find it difficult to win ground among cloud service providers, who are often risk-averse; therefore, public bodies should take the lead in adopting these technologies.

10. Infrastructure and Technology (policy recommendations 1&3)
11. Quantum Technology (PA 1): one participant argued that it is misleading to interconnect quantum technology with classic HPC or put it in the HPC context because it is still highly experimental.
12. There was a suggestion that the continuum requires targeted focus areas.
13. Interoperability between edge, cloud and IoT was identified as essential and should be a top priority for the Continuum to function properly.
14. General strategic concerns
15. Dependence on non-EU Hyperscalers was highlighted as a direct threat to the security and resilience of the EU tech landscape.
16. Economic barriers: high energy costs were cited as a factor that limits the ability to expand IT infrastructure.

5.3 Input from the international perspective

The analysis of Canada, India, Japan, New Zealand and the Republic of Korea confirms that the policy challenges identified in NexusForum.EU are not unique to Europe, but part of a broader international transition towards more sovereign, interoperable and AI-enabled computing ecosystems. Across the five countries, the most consistent patterns are the same: dependence on US hyperscalers, concern about vendor lock-in, pressure to strengthen public-sector digital sovereignty, and growing interest in trusted data-sharing, open standards and domestic capability-building.

Several lessons emerge for the European policy package. First, the international cases show that cloud-first and AI adoption **policies are most effective when they are paired with concrete governance mechanisms, procurement rules and certification schemes**. This is particularly visible in Japan's emphasis on interoperability and vendor-neutral reference architectures, and in South Korea's use of CSAP as a gatekeeping mechanism for public-sector cloud adoption. These experiences support the relevance of Policy Recommendations on trust, interoperability, governance and strategic autonomy, and suggest that Europe could further strengthen its approach through clearer compliance pathways, certification and procurement conditions.

Second, the country analyses underline the importance of combining digital sovereignty with practical adoption measures. Canada and New Zealand both show that public-cloud modernisation can proceed quickly, but that without a broader sovereignty strategy it remains largely dependent on foreign providers and may not extend to the edge, IoT or wider SME ecosystem. India, by contrast, illustrates the value of a strong digital public infrastructure model, especially through its open API-based IndiaStack and its emerging sovereign cloud and semiconductor policies, but also shows that fragmentation in privacy, data governance and innovation support can limit the coherence of the overall approach. For Europe, this reinforces **the need to connect infrastructure policy with SME support, skills, and market-shaping measures**.

Third, the international evidence points to a shared interest in open standards, data spaces and federated interoperability. Japan's DATA-EX and Ouranos Ecosystem, South Korea's

Co-funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

sectoral platform approach, and India's interest in stronger data governance all show that data sharing and portability are becoming central policy concerns, even if the institutional models differ. This creates a **clear opportunity for EU cooperation on standards, reference architectures and cross-border interoperability,** especially where policy goals overlap around trustworthy AI, industrial digitalisation and sector-specific data sharing.

Fourth, the analyses suggest that semiconductor, edge and network capabilities are increasingly treated as strategic enablers rather than isolated industrial topics. South Korea's integrated 6G, AI and semiconductor strategy, Japan's focus on edge-AI chips and smart city architectures, and India's semiconductor mission all show that hardware, networks and AI deployment are now being planned together. This supports the idea that the European policy package could benefit from **a stronger link between continuum policy and industrial policy, especially in relation to chips, edge systems and advanced connectivity**.

Finally, the international perspective indicates clear opportunities for collaboration. Canada, Japan and New Zealand are already closely aligned with the EU through Horizon Europe association, adequacy arrangements or trade cooperation, while Japan and the Republic of Korea are active partners in data spaces, AI safety and standards-oriented cooperation. India is a more complex partner, but its scale, semiconductor ambitions and interest in sovereign digital infrastructure make it strategically relevant for future cooperation. Overall, the five-country analysis suggests that the **EU can strengthen its policy package** not only **by adding international cooperation** as a cross-cutting dimension, but also **by sharpening support for interoperable architectures, trusted cloud adoption, open standards and digital sovereignty partnerships**.

Main findings from NexusForum EU-Japan and EU-Korea events

From the EU-Korea event in 2026, discussions show a strong shared direction on the computing continuum: both sides favor interoperable, federated data flows, open standards, and joint pilots over rigid data localization or vendor lock-in. The overall message is that EU and South Korea are increasingly aligned on building trusted cloud-edge-IoT-AI infrastructure through common governance, collaborative testbeds, and talent exchange, with a clear focus on sovereignty plus practical deployment.

From the EU-Japan Summit held in 2025, a similar message can be shared but a bit sharper on open ecosystems and federation. The survey done in the event shows strong support for free data flows with trust, more and diverse data for AI, and especially an alternative to hyperscaler lock-in based on an open ecosystem of many smaller providers, while the rapporteur notes broad agreement on interoperability, data spaces, open source approaches, and aligned funding and procedures for joint projects. The overall conclusion is that policy alignment is not just about easing data movement, but about creating a federated, interoperable infrastructure that supports innovation, competitiveness, and mutual trust.

5.4 The final policy roadmap for the Cognitive Computing Continuum: Policy related recommendations

This section presents the consolidated final Policy Recommendations for the European Cognitive Computing Continuum. These recommendations are the result of an iterative and participatory refinement process, evolving from an initial draft into a comprehensive strategic framework.

To ensure that the final proposals are robust, evidence-based, and aligned with the needs of the ecosystem, the primary draft was subjected to multiple layers of validation and enrichment.

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

This process integrated quantitative and qualitative feedback derived from a comprehensive EU-wide survey on strategic gaps, expert deliberations during a dedicated Policy Recommendations workshop, and high-level stakeholder consultations conducted during the NexusForum.EU Summits in Japan and the Republic of Korea.

Furthermore, the recommendations have been cross-referenced with international landscape reports to ensure that the European approach is both globally competitive and strategically aligned with like-minded partners. The resulting framework aims to address critical structural deficiencies while providing actionable pathways to enhance Europe's digital sovereignty and technological leadership.

Each Policy Recommendation is presented following a common structure. It starts with a strategic goal, then identifies the specific gaps it is intended to address and finally sets out a set of Strategic Actions that indicate the main implementation levers. These actions cover different types of intervention, including regulatory and governance measures, funding and financial instruments, public procurement, standards and open source approaches, skills and capacity building, and international cooperation. The Strategic Actions are indicative building blocks rather than an exhaustive list of measures and are designed to guide the subsequent design of concrete instruments and programmes. The seven Policy Recommendations are detailed below.

5.4.1 Policy Recommendation 1: Unify the Fragmented Infrastructure and Integrate Future Technologies

Strategic goal: Establish a federated, energy-efficient Cognitive Computing Continuum that seamlessly integrates cloud, edge, IoT, and emerging quantum resources, consolidating fragmented infrastructures into a coherent European strategic asset.

Addressed gaps: Gap 2 (Fragmented Infrastructure Ecosystem), Gap 8 (Infrastructure Fragmentation and Energy Costs), Gap 9 (Lack of Quantum HPC Integration Strategy).

Strategic Actions:

- **Establish a ‘Federation by Design’ mandate** for all EU co-funded digital infrastructures (HPC, cloud, edge, networking) requiring the adoption of a common reference architecture for the European Continuum Fabric to ensure native interoperability and cross-border scalability.
- **Prioritise Energy-Efficient AI Infrastructure**: Integrate specific targets for carbon-emissions-aware computing and energy-efficient data centre operations.
- **Develop Joint International R&D Testbeds**: Create shared R&D and testbeds with strategic partners (e.g., Republic of Korea) enabling collaborative innovation while maintaining strict national sovereignty over sensitive public data.
- **Continuum-ready certification and testbeds**: Reserve a share of infrastructure budgets for interoperability testing labs and introduce a “Continuum-Ready” certification covering APIs, data models and federation services as a prerequisite for EU supported deployments.
- **Establish a hybrid quantum–HPC roadmap**: Develop a dedicated policy framework defining interfaces, reference architectures and shared testbeds for integrating quantum accelerators with classical HPC and edge nodes, so that quantum capabilities are embedded into the continuum rather than developed in isolation.

- **Establish a Quantum–Continuum integration testbed**: Create shared European laboratories and facilities (building on EuroHPC infrastructure) where quantum accelerators are physically integrated with edge HPC clusters, enabling researchers and developers to prototype, test and validate hybrid quantum classical algorithms in a realistic continuum environment. Fund joint governance between quantum computing centres and edge compute operators to ensure seamless technical integration.

- **Photonics ready infrastructure standard**: Extend the "Continuum-Ready" certification to include photonic (optical) computing architectures alongside quantum and classical HPC, ensuring that emerging photonic accelerators for AI and data processing can be deployed and federated within the continuum without proprietary lock-in.

- **Align infrastructure funding with green connectivity objectives**: Condition EU and national support for connectivity and data centres on the deployment of energy efficient fibre and 5G/6G networks explicitly designed to support decentralised edge workloads and encourage projects that demonstrate measurable improvements in energy per compute through advanced cooling, dynamic power management and the use of renewable powered data centres.

5.4.2 Policy Recommendation 2: Strengthen Trust and Cross-Border Data Fluidity

Strategic goal: Position European cloud-edge-data solutions as the global benchmark for trust by facilitating secure cross-border data flows and embedding sovereignty, security, and regulatory compliance into the core of the continuum.

Addressed gaps: Gap 1 (Technological Sovereignty Challenges), Gap 4 (Low Confidence in EU Cloud Providers), Gap 5 (Barriers to Cross-Border Data Sharing).

Strategic Actions:

- **Implement a mechanism for the alignment of national regulations,** with EU-level data sharing principles to resolve structural bottlenecks caused by fragmented jurisdictional implementations.

- **Harmonise the regulatory framework for data spaces**, implementing targeted guidance to eliminate divergent national interpretations of data-sharing rules and promoting the use of open source reference implementations for data-exchange protocols.

- **Develop a "Trusted European Cloud and Edge" label**: Build on existing EU work on trusted cloud frameworks to create a tiered label that combines requirements on European ownership and control, insulation from extra territorial data access laws, robust cybersecurity and alignment with EU data protection rules, and promote its uptake in public and private procurement.

- **Integrate security and sovereignty by design into procurement**: Require that public sector and critical infrastructure tenders systematically prioritise solutions with demonstrable data localisation options, transparent security assurance and technical reversibility over opaque foreign platforms.

- **Support independent audit services**: Facilitate EU level audits as service facilities that certify compliance of cloud and edge-based services with trusted cloud and data space requirements, providing ready to use assurance for public buyers and SMEs.
- **Move beyond bilateral data corridors** toward the creation of 'Global Sovereign Federation Zones' with aligned partners (Japan, South Korea, Canada, New Zealand), utilising joint reference architectures and shared certification schemes to enable the seamless movement of workloads and data while respecting mutual sovereignty.
- **Promote reference implementations and flagship deployments**: Fund demonstrator projects in key sectors (manufacturing, health, mobility, energy, smart cities).
- **Support responsible AI and trust frameworks**: Integrate AI safety, ethics, and transparency frameworks into deployments.

5.4.3 Policy Recommendation 3: Reduce Vendor Lock-In and Strengthen Strategic Autonomy

Strategic goal: Significantly reduce the structural dependence of European SMEs and public bodies on (non-EU) technology vendors by enforcing interoperability and building a resilient, federated ecosystem of diverse European providers underpinned by open standards, avoiding the replication of the hyperscaler model in favour of a distributed, sovereign architecture.

Addressed gaps: Gap 7 (SME Dependence on Non-EU Hyperscalers), Gap 13 (Vendor Lock-In Risks), Gap 14 (Semiconductor Supply Chain Weaknesses).

Strategic Actions:

- **Enforce the 'Right to Switch' through mandatory contractual clauses** in publicly supported contracts, ensuring data portability and technical reversibility to mitigate structural vendor lock-in.
- **Provide targeted incentives for multi-provider strategies**: Supporting the adoption of multi-cloud and multi-edge architectures to reduce single-vendor exposure.
- **Publish multi-provider reference architectures**: Develop and promote open multi cloud and multi edge blueprints, based for example on container orchestration and open service mesh technologies and aligned with IPCEI CIS reference architectures, to lower the entry barrier for SMEs.
- **Establish a cross-sectoral Industrial-Continuum Taskforce** to align the European Chips Act and connectivity strategies (6G) directly with the Computing Continuum's software and orchestration layers, ensuring that hardware development is driven by the specific requirements of federated, sovereign cloud-edge architectures.
- **Increase transparency and resilience in the supply chain**: Encourage traceability mechanisms and diversified sourcing for critical components used in continuum infrastructures supported by EU funds, improving risk management for public authorities and industry.
- **Shift strategic positioning from "Competing with Hyperscalers" to "Challenger Positions"**: Focus on trusted computing and federated architectures where Europe possesses a comparative advantage, rather than attempt to replicate the volume of non-EU hyperscalers.

Co-funded by the European Union
Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

5.4.4 Policy Recommendation 4: Consolidate Governance and Coordination for the Continuum

Strategic goal: Provide coherent strategic governance for the Cognitive Computing Continuum by aligning fragmented initiatives, optimizing coordination across funding instruments, and ensuring the consistent engagement of industry and SMEs.

Addressed gaps: Gap 10 (Ineffective Coordination of Strategic Initiatives), Gap 7 (SME Dependence on Non-EU Hyperscalers – via weak engagement), Gap 11 (Limited SME Participation in Global Ecosystems).

Strategic Actions:

- **European Continuum Governance Mechanism**: Establish a European Continuum Coordination Board as a dedicated governance structure designed to steer the implementation of continuum-related policies and guarantee strategic continuity beyond the lifecycles of individual projects.
- **Strategic Initiative Alignment Protocol**: Implement a formal coordination process to ensure operational and strategic alignment between major initiatives—such as IPCEI-CIS, Gaia-X, and IDSA—utilising shared roadmaps and joint KPIs to eliminate redundancies and optimise resource allocation
- **SME-Industry Integration Framework**: Establish a structured mechanism to bridge the gap between academic research and industrial application by requiring the active involvement of SMEs and sectoral users (such as those in manufacturing, health, mobility, and energy) in the design and evaluation of continuum-related projects, while simultaneously mandating that Research and Technology Organisations (RTOs) and universities share open source technology and data with SMEs and large enterprises as a precondition for funding.

5.4.5 Policy Recommendation 5: Strengthen the Open Source and Standards Commons

Strategic goal: Transform Europe's open source and standards assets into a robust industrial common that underpins digital sovereignty and accelerates innovation across the computing continuum.

Addressed gaps: Gap 6 (Weak Open Source Ecosystem), Gap 1 (Technological Sovereignty Challenges), Gap 10 (Ineffective Coordination of Strategic Initiatives).

Strategic Actions:

- **Establish a sovereign open source and standards facility:** dedicated to the long-term maintenance, security, hardening, and industrial evolution of critical continuum components.
- **Promote open by default research outputs**: Require that software, reference architectures and core libraries developed with EU R&I funding for the continuum be made available under suitable open licenses, accompanied by documentation and governance models that facilitate industrial uptake.
- **Transition toward an 'Industrial Open Source' model**, incentivising the creation of professional support entities to provide industrial-grade maintenance and services, moving beyond purely community-driven models.

- **Support skills for open source**: Promote training and capacity building programmes that enable developers, integrators and public administrations to effectively use and contribute to open source technologies relevant for the continuum.

- **Implement incentive schemes** to encourage large-scale industry participation and contribution to the open source commons.

5.4.6 Policy Recommendation 6: Support SMEs to Scale and Compete Globally

Strategic goal: Eliminate structural regulatory and financial barriers that impede the scaling of European deep-tech SMEs and enhance their integration into global digital value chains.

Addressed gaps: Gap 3 (Regulatory Complexity for SMEs), Gap 11 (Limited SME Participation in Global Ecosystems), Gap 12 (Funding Gaps and SME Vulnerability), Gap 7 (SME Dependence on Non-EU Hyperscalers).

Strategic Actions:

- **Institute a framework of 'Green Lane Regulatory Pathways'** and cross-border regulatory sandboxes to provide SMEs with a simplified, one-stop-shop compliance mechanism for the AI Act and Data Act.

- **Deploy targeted financial instruments**, including blended-finance schemes and a dedicated European AI Venture Fund managed by the EIF, to support capital-intensive deep-tech scaling.

- **Strengthen scale up finance for cognitive technologies**: Develop targeted financial instruments (for example blended finance schemes, growth funds or guarantees) dedicated to capital intensive continuum technologies, reducing early dependence on foreign investment and acquisitions.

- **AI-ready-SME certification programme**: Establish a tiered certification scheme that recognizes SMEs and startups developing open source AI stack components, reference implementations or continuum native solutions. Certified SMEs should receive priority access to EU funding (Horizon, Digital Europe Programme), preferential scoring in public procurement tenders and visibility in a searchable "European AI Tech Register", creating a market advantage for open stack contributors.

- **Facilitate SME participation in global ecosystems**: Support SMEs and research actors in engaging with international standardisation bodies and global innovation networks (such as ISO, IEC, IEEE or relevant open technology foundations), ensuring that European continuum architectures and protocols are represented and adopted.

- **Provide a one-stop-support interface**: Create a “Continuum SME Hub” offering guidance on regulation, funding opportunities, standardisation and internationalisation for companies developing or deploying continuum solutions.

- **Reform EU funding application processes for SMEs** to reduce administrative complexity, favouring simpler application formats and more accessible award sizes to increase participation rates.

- **Implement 'Sovereign Migration Grants'** specifically for SMEs to transition from proprietary foreign cloud stacks to the European Federated Continuum, ensuring that digital transformation is paired with a reduction in structural dependency.

5.4.7 Policy Recommendation 7: Enhance Technological Sovereignty and Adoption Capacity

Strategic goal: Increase Europe's capacity to develop, deploy, and govern advanced technologies across the continuum while reinforcing systemic trust in AI and data driven solutions.

Addressed gaps: Gap 1 (Technological Sovereignty Challenges), Gap 4 (Low Confidence in EU Cloud Providers), Gap 6 (Weak Open Source Ecosystem).

Strategic Actions:

- **Implement comprehensive upskilling and capability-building programmes** targeting public administrations and SMEs in the domains of cloud-edge-IoT-AI and open source tools.
- **Support responsible AI and trust frameworks**: Encourage the integration of AI safety, ethics and transparency frameworks into continuum deployments, building on ongoing European and international work on trustworthy AI to foster user trust and acceptance.
- **Develop a European equivalent to the CSAP model** (Cloud Security Assurance Program), establishing mandatory cybersecurity and sovereignty certification criteria that act as a prerequisite for any provider, whether European or not, seeking to host critical public-sector workloads.
- **Fund large-scale reference implementations and flagship deployments** in strategic sectors (e.g., health, energy, mobility) to showcase the viability of sovereign, interoperable solutions.

5.4.8 Alignment with Research & Innovation roadmap

The seven Policy Recommendations developed in NexusForum.EU are closely aligned with the **six Strategic Destinations defined in the Research & Innovation Roadmap** for the European Cognitive Computing Continuum. The relationship between both frameworks is not one-to-one: the Strategic Destinations describe the long-term outcomes that European research and innovation should enable, while the Policy Recommendations translate those outcomes into policy-oriented levers and implementation measures.

The Strategic Destinations for Europe, as set out in the Research & Innovation Roadmap deliverable, are:

- Destination 1: Scalable and energy-efficient AI and data processing
- Destination 2: An AI stack built on an open European hardware and computing ecosystem
- Destination 3: A competitive European AI and machine learning ecosystem
- Destination 4: Secure, sovereign, and interoperable European computing capabilities
- Destination 5: Advanced digitalisation and AI adoption in industry and public sectors
- Destination 6: European leadership in disruptive and emerging computing paradigms

Policy Recommendations and strongest destination links

Policy Recommendation	Dest 1	Dest 2	Dest 3	Dest 4	Dest 5	Dest 6
1. Fragmented infrastructure and future technologies	**Strong**	Medium	Medium	**Strong**	Medium	**Strong**
2. Trust and cross-border data fluidity	Medium		Medium		**Strong**	**Strong**
3. Vendor lock-in and strategic autonomy		**Strong**		**Strong**	Medium	
4. Governance and coordination			Medium	**Strong**	**Strong**	
5. Open source and standards commons		**Strong**	Strong	**Strong**		
6. SME scale-up and global competitiveness		Medium	**Strong**		**Strong**	
7. Technological sovereignty and adoption capacity			**Strong**	**Strong**	**Strong**	

Table 6. Policy Recommendations and strongest destination links

Taken together, Policy Recommendations provide a coherent policy backbone for the Strategic Destinations. Recommendations 1, 2 and 3 mainly underpin Destinations 1, 2, 4 and 6 by focusing on infrastructure federation, open and sovereign computing capacity, vendor lock-in reduction and the integration of emerging technologies such as quantum and advanced edge AI. Recommendations 4 and 5 strengthen the enabling environment for these outcomes by improving governance, coordination, open source ecosystems and standardisation, which are essential for secure, interoperable and trusted continuum capabilities.

At the same time, Recommendations 6 and 7 primarily support Destinations 3 and 5 by addressing SME scale-up, skills, adoption capacity and flagship deployments in industry and the public sector, while also contributing to sovereign and interoperable capabilities under Destination 4. This multi-alignment is consistent with the roadmap itself, which frames the Strategic Destinations as mutually reinforcing outcomes rather than separate workstreams, and confirms that each Policy Recommendation contributes to at least one destination and that each destination is supported by at least one Policy Recommendations.

This confirms that the policy package and the R&I Roadmap are mutually consistent: the roadmap identifies the desired European outcomes, while the Policy Recommendations provide the enabling interventions needed to move towards them.

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

5.4.9 Summary

The proposed framework aims to unify Europe's fragmented cloud-edge-IoT resources into a coherent, energy-efficient strategic asset through a 'Federation by Design' mandate and harmonised regulatory frameworks for data spaces. This structural integration is underpinned by a new governance model, including a European Continuum Coordination Board, designed to align major initiatives and ensure strategic continuity beyond individual project lifecycles.

Simultaneously, the strategy reinforces digital sovereignty by reducing vendor lock-in via the 'Right to Switch' and transitioning towards an 'Industrial Open Source' model supported by a dedicated sovereign facility. To ensure sustainable adoption, the roadmap prioritises large-scale flagship deployments and comprehensive upskilling programmes, empowering SMEs and public bodies to deploy secure, interoperable, and sovereign solutions across strategic sectors.

Co-funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

6. Future outlook

The findings and recommendations presented in this report provide a foundational roadmap for the EU Cognitive Computing Continuum. However, the rapid evolution of generative AI, quantum computing, and edge-native architectures suggests that the policy landscape must remain dynamic. To ensure the long-term success of the strategic goals outlined in D3.3, the following future trajectories are envisioned:

- **Continuous Regulatory Evolution**: As the EU continues to implement the AI Act and the Data Act, the focus must shift from *establishing* regulations to *optimizing* their application. Future efforts should prioritize the creation of "regulatory sandboxes" specifically for the Computing Continuum, allowing SMEs and research centres to test cross-border data fluidity and edge-cloud integration in a controlled, compliant environment.
- **Scaling the Open Source Commons**: The maturity gap identified between the automotive and agriculture sectors indicates that the "Open Source" model is not one-size-fits-all. The future outlook involves the creation of sector-specific open source foundations that provide standardized, sovereign building blocks for various industrial verticals, thereby accelerating the transition from experimental pilots to industrial-scale adoption.
- **Strengthening International Policy Alliances**: The comparative analysis of Japan, ROK, Canada, New Zealand, and India suggest a growing global trend toward "digital sovereignty." Future strategic efforts should focus on establishing "Sovereignty Partnerships", inter-governmental agreements that align standards and certifications, allowing the EU to export its values of trust and privacy while importing technical efficiencies from global partners.
- **From Policy Recommendations to Legislative Action**: The seven Policy Recommendations proposed in this report are intended to serve as catalysts. The ultimate goal is the integration of these recommendations into future Digital Sovereignty framework targets, ensuring that the Cognitive Computing Continuum is supported by dedicated funding mechanisms and streamlined governance structures

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

Conclusions

Deliverable D3.3, “Digital Policy Report – c”, concludes a comprehensive effort to map, analyse, and influence the policy landscape of the EU Cognitive Computing Continuum. Through a systematic evaluation of the regulatory environment, this report has demonstrated that achieving true digital sovereignty requires more than technical excellence; it demands a synchronized policy framework that aligns research, innovation, and regulation.

The project's analysis has highlighted a critical intersection between regulatory agility and technological autonomy. By expanding the scope to include international perspectives from Japan, ROK, Canada, New Zealand, and India, the report has provided a global benchmark that reveals both the strengths and the vulnerabilities of the European approach. Furthermore, the investigation into Open Source (OS) and Open Standards, specifically the comparative analysis between the Automotive and Agriculture sectors, underscores that OS is a fundamental strategic asset for reducing vendor lock-in and ensuring the long-term viability of the Continuum.

The methodology employed in this deliverable ensured that the final policy recommendations were not merely theoretical but were grounded in technical evidence and stakeholder validation. By identifying 14 critical gaps and translating them into seven strategic Policy Recommendations, the project has provided a concrete roadmap for unifying fragmented infrastructures, strengthening data fluidity, and empowering European SMEs to compete on a global scale.

In summary, the findings of D3.3 provide the necessary evidence base to move toward a more integrated and sovereign Cognitive Computing Continuum. The transition from analysis to action, facilitated by the developed Policy Briefs and the strategic roadmap, establishes a foundation upon which the EU can build a resilient, open, and autonomous digital ecosystem.

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

References

[1] European Commission, “Joint Communication: International Digital Strategy for the EU,” 2025. [Online]. Available: https://ec.europa.eu/newsroom/dae/redirection/document/116454 . [Accessed 29 04 2026].

[2] NexusForum.EU Consortium, “D3.1 Digital Policy Report - a,” 2024.

[3] NexusForum.EU Consortium, “D2.2 Research & Innovation Roadmap - b,” 2024.

[4] European Commission, “Annex I: New initiatives, COM(2025) 45 final - Commission Communication 'Commission work programme 2025',” 2025.

[5] European Commission, “nnex 1 to the Joint Communication: International Digital Strategy for the EU,” 2026. [Online]. Available: https://ec.europa.eu/newsroom/dae/redirection/document/116453 Accessed 29th April 2026. [Accessed 29 05 2026].

[6] European Commission, “Cloud Sovereignty Framework (version 1.2.1, October 2025,” 10 2025. [Online]. Available: https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf. [Accessed 27 05 2026].

[7] EDPS, “European Data Protection Supervisor Annual Report,” 2024. [Online]. Available: https://www.edps.europa.eu/system/files/2025-04/edps_annual_report-2024_en.pdf . [Accessed 11 05 2026].

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

Annex – Final set of policy briefs

The findings presented in this deliverable are expanded upon in a series of NexusForum.EU Policy Briefs available via the project's official website. These standalone documents offer an in-depth exploration of specific thematic areas, ranging from detailed national landscape studies (Canada, India, Japan, New Zealand, and South Korea) and a comprehensive Comparative Analysis, to the extended version of the SWOT analysis presented previously in this deliverable. To ensure the findings reach a broader stakeholder audience, the series also includes a condensed Policy Recommendations brief, which distils complex technical analysis into graphic based summary.

International landscape: CANADA

International landscape: INDIA

International landscape: JAPAN

International landscape: NEW ZEALAND

International landscape: SOUTH KOREA

International landscape: COMPARATIVE ANALYSIS

SWOT Analysis

Policy Recommendations Policy Brief

Co-funded by the European Union

Project funded by Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Swiss Confederation Federal Department of Economic Affairs, Education and Research EAER State Secretariat for Education, Research and Innovation SERI

