



## D3.2 Digital Policy Report - b

*Revision: v.1.0*

Work package	WP3	Task	Task 3.1/3.2/3.3/3.4/3.5
Submission date	30/06/2025	Due date	30/06/2025
Deliverable lead	TECNALIA	Version	1.0
Authors	Javier Mendibil, Virginia Castaños, Enrique Areizaga, Juncal Alonso, Olatz Ibañez, Josu Diaz de Arcaya (Tecnalia), Chiara Zincone (OpenNebula Systems), Francesco Panella (Martel), Sachiko Muto, Johan Linaker (RISE), Danijel Pavlica (F6S), Tajana Medaković Dautović (F6S), Andrew Adams, Kiyoshi Murata (Meiji University).		
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 to be produced in M18 and M30.
Keywords	Regulatory framework, policy, Open Source, standardisation, skills, digital sovereignty.

## DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V0.1	28/02/2025	1st version of the TOC for comments	Juncal Alonso (Tecnalia)
V0.2	24/03/2025	Agreed version of the TOC. Ready to start editing.	All
V0.3	18/04/2025	Included content in section 2,3 and 5	Francesco Panella (Martel) Chiara Zincone (OpenNebula) Javier Mendibil, Cristina Castaños, Enrique Areizaga, Olatz Ibañez (TECNALIA) Tajana Medaković, Danijel Pavlica (F6S)
V0.4	28/04/2025	Included content in section 4	Sachiko Muto (RISE)
V0.5	07/05/2025	Included content in section 2	Juncal Alonso (Tecnalia)
V0.6	09/05/2025	Updated Executive Summary and Introduction, included content in 5.1.3.1	Juncal Alonso, Javier Mendibil, Virginia Castaños (Tecnalia)
V0.7	12/05/2025	Updated section 4	Sachiko Muto (RISE) Juncal Alonso (Tecnalia)
V0.8	07/06/2025	Updated section 6	Giacomo Inches (Martel), Andrew Adams (Meiji University), Sachiko Muto (RISE)
V1.0	20/06/2025	Addressed comment from internal review. Final version creation	All

## Disclaimer

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the other granting authorities. Neither the European Union nor the granting authority can be held responsible for them.

## Copyright notice

© 2024 - 2026 NexusForum.EU Consortium

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
SEN	Sensitive, limited under the conditions of the Grant Agreement	
Classified R-UE/ EU-R	EU RESTRICTED under the Commission Decision No2015/ 444	
Classified C-UE/ EU-C	EU CONFIDENTIAL under the Commission Decision No2015/ 444	
Classified S-UE/ EU-S	EU SECRET under the Commission Decision No2015/ 444	

- \* R: Document, report (excluding the periodic and final reports)  
 DEM: Demonstrator, pilot, prototype, plan designs  
 DEC: Websites, patents filing, press & media actions, videos, etc.  
 DATA: Data sets, microdata, etc  
 DMP: Data management plan  
 ETHICS: Deliverables related to ethics issues.  
 SECURITY: Deliverables related to security issues  
 OTHER: Software, technical diagram, algorithms, models, etc.

## Executive summary

Deliverable **D3.2 “Digital Policy Report – b”** is the second one of a series of three (scheduled for M9, M18, and M30), describing the approach and the activities performed in the Project to support the European computing constituency by monitoring the European regulatory landscape and policy initiatives related to the Cognitive Computing Continuum.

This **second version of the Digital Policy Report** offers a more in-depth overview of the implications of the most relevant regulations and policies for both the scientific and industrial ecosystems. It analyses their impact on various technology topics and highlights the main takeaways from upcoming policy developments. Additionally, the report proposes ways to align research and technology priorities across the continuum through an in-depth analysis of six key factors i.e., F1: Technology, innovation and research capabilities, F2: Framework conditions (policies, strategies, plans, regulations, etc.), F3: Enabling conditions (Open Source, open standards, skills and ethics), F4: Infrastructures and connectivity (including space infrastructure and data), F5: Collaboration & engagement between initiatives at EU and international level, and F6: Industry participation. It also identifies initiatives open to participation for the NexusForum.EU community. Finally, it examines additional dimensions such as open source, standardization, and skills in the context of European sovereignty, and compiles initial insights from the international landscape toward achieving Digital Sovereignty in Europe.

During the second period (M10-M18), the analysis carried out of the European policy and regulatory landscape within the Computing Continuum reveals that several strategic areas need to be addressed to achieve consolidation and technological sovereignty. Some of the key findings include:

1. A report providing a forward-looking analysis of major policy initiatives currently in the pipeline. Including the mapping of the European policy and regulatory landscape within the Computing Continuum, with a special focus on analyzing—clearly and accessibly—the impact of each selected regulation on key technological topics (chosen from the NexusForum.EU research and innovation roadmap).
2. A Strategy to raise awareness of and encourage meaningful participation in policy initiatives—particularly those led by the European Commission. This strategy is based on two interconnected approaches: enhancing involvement in formal public consultations and supporting participatory, co-creative activities that contribute to a more proactive and inclusive policy development process.
3. Implementation of the second phase of the proposed methodological approach to derive policy-related recommendations aimed at strengthening EU sovereignty in the Computing Continuum. During this phase, NexusForum.EU has identified key gaps through a SWOT analysis of the six key factors based on information gathered from various tasks within the project and from online workshops held with task leaders and relevant partners. The outcomes of the SWOT analysis highlight the main gaps in each factor, which will be further discussed, contrasted with, and validated in the Working Groups. It is from these identified gaps that the project will formulate concrete policy recommendations. Preliminary findings from the SWOT analysis state that the EU computing continuum must focus on several strategic areas to achieve consolidation and technological sovereignty. First, developing a Federated Technologies Ecosystem across edge, cloud, and IoT will enhance resource utilization, collaboration, and digital sovereignty while improving competitiveness. Second, implementing the European Data Strategy by creating a single market for data and Common European Data Spaces will promote innovation, data sovereignty, and market growth. Third, a coordinated strategy for open-source maintenance, scalability, and skills development is essential to overcome fragmentation and ensure a sustainable computing ecosystem. Fourth, building a unified, open, and

secure digital infrastructure will support AI factories and their integration with High-Performance Computing, fostering innovation across key sectors. Fifth, strategic cooperation with like-minded countries such as Japan, South Korea, and Canada can strengthen cloud and edge infrastructure and counter dependency on non-European hyperscalers. Sixth, a new EU semiconductor strategy is critical to address supply chain vulnerabilities and support SMEs in the Cognitive Computing Continuum. Lastly, simplifying and harmonizing digital regulations will reduce fragmentation, lower compliance costs, and enable a more competitive and innovative Digital Single Market across Cloud, Edge, and IoT.

4. Additionally, the analysis highlights the importance of:

- **Open-Source Software (OSS) in Digital Sovereignty:** OSS plays a crucial role in enabling digital sovereignty, particularly in sectors like Agriculture.
- **International Cooperation:** The EU-Japan Digital Week in Tokyo and related events like the Japan Workshop in Brussels demonstrate the value of strategic cooperation with countries like Japan in areas like cloud and edge infrastructure.

These findings provide a foundation for concrete policy recommendations aimed at strengthening EU sovereignty in the Computing Continuum.

## Table of contents

<b>DOCUMENT REVISION HISTORY .....</b>	<b>2</b>
<b>Disclaimer .....</b>	<b>2</b>
<b>Copyright notice.....</b>	<b>2</b>
<b>Executive summary.....</b>	<b>4</b>
<b>Table of contents.....</b>	<b>6</b>
<b>List of figures .....</b>	<b>8</b>
<b>List of tables .....</b>	<b>9</b>
<b>Abbreviations .....</b>	<b>10</b>
<b>1 Introduction.....</b>	<b>11</b>
<b>2 Mapping European policy and regulatory landscape in the computing Continuum .....</b>	<b>12</b>
2.1 The policy-technology matrix .....	12
2.1.1 The impact of selected EU policy and legal instruments along the Computing Continuum	13
2.2 Initiatives and Stakeholders .....	27
2.3 Future Outlook .....	28
2.3.1 Upcoming EU policies meant to shape technology .....	28
2.3.2 Upcoming initiatives meant to shape technology.....	34
2.3.3 Simplification and Implementation .....	35
<b>3 Increasing the awareness and participation in policy initiatives of the Cognitive Computing Continuum.....</b>	<b>38</b>
3.1 NexusForum.EU approach for increasing awareness on Cognitive Computing Continuum policy initiatives.....	38
3.2 Identified public open consultations .....	39
<b>4 EU Open Source, Standardisation, and Skills Development initiatives .....</b>	<b>42</b>
4.1 Case Study: Open Source in Agriculture .....	42
4.2 Empowering Digital Sovereignty: The Role of a Skilled Open Source Workforce and the EU Open Source Academy .....	45
4.3 Standards .....	46
<b>5 Suggestion of new policy initiatives and decisions: Analysing the factors ...</b>	<b>47</b>
5.1 Co-creating the SWOT Analysis .....	47
5.1.1 Analytical Approach and Implementation Process .....	47
5.1.2 SWOT Dimensions.....	47
5.1.3 Results of swot analysis.....	48
5.1.4 Next steps .....	57
<b>6 Digital Sovereignty in the international context .....</b>	<b>59</b>
<b>Conclusions.....</b>	<b>61</b>
<b>References.....</b>	<b>63</b>
<b>Annex 1 – EUCloudEdgeIoT.eu Digital policies visualisation .....</b>	<b>64</b>



## List of figures

Figure 1 - Excerpt 1 of the interactive policy matrix on the EUCloudEdgeIoT.eu website.....	12
Figure 2. Excerpt 2 of the interactive policy matrix on the EUCloudEdgeIoT.eu website .....	13
Figure 3. Initiatives collected in EUCEI web page. ....	28
Figure 4. R&D initiatives mapped to the NexusForum.EU. R&D roadmap topics.....	35
Figure 5. Whaller publication of one online consultation.....	41
Figure 6. SWOT analysis for F1-Technology, innovation and research capabilities.....	49
Figure 7. SWOT analysis for F2 Framework conditions (policies, strategies, plans, regulations, etc.)- 50	
Figure 8. SWOT analysis for F3 Enabling conditions (Open Source, open standards, skills and ethics)- 51	
Figure 9. SWOT analysis for F4 Infrastructures and connectivity (including space infrastructure and data)- .....	52
Figure 10. SWOT analysis for F5 Collaboration & engagement between initiatives at EU and international level.....	53
Figure 11. SWOT analysis for F6 Industry participation.....	54
Figure 12 - eucloudedgeiot.eu - Policies and initiatives interactive visualisation in the EUCEI webpage 64	



## List of tables

Table 1. Upcoming EU policies, as outlined in the Commission Work Programme 2025 [3] .....	29
Table 2. Policy related open consultations .....	40
Table 3. SWOT Analysis dimensions .....	48

## Abbreviations

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

# 1 Introduction

Deliverable **D3.2 “Digital Policy Report – b”** is the second one of a series of three (M9 [1], **M18**, M30), describing the approach and activities undertaken in the Project to raise awareness among the European computing community about the latest policy-related initiatives affecting the NeexusForum.eu community. These activities include monitoring the European regulatory landscape and policy initiatives related to the Cognitive Computing Continuum, offering an up-to-date and factual overview of the implications for the scientific and industrial ecosystems, and suggesting ways to align research and technology priorities in key strategic areas with relevant policy aspects. NexusForum.EU aims also at promoting the participation of EU organisations in the policy definition and feedback process and implementing the analysis on the impact of the Regulatory Framework towards Digital European Sovereignty in the Cognitive Computing Continuum.

Overall, the policy-related activities in NexusForum.EU are structured around five key pillars:

1. Understanding and mapping the European regulatory landscape in the context of the Computing Continuum;
2. Increasing awareness and fostering participation in policy-related initiatives;
3. Analyzing the needs and impacts related to Open Source, standardization, and skills;
4. Proposing future policy initiatives; and
5. Analyzing the international policy and technology landscape."

The remaining content of the current report is structured in the following sections:

- Section 2 outlines the methodology and activities conducted to map the European policy and regulatory landscape in relation to the technology topics of the EU Computing Continuum, based on the latest version of the NexusForum.EU R&D roadmap [2]. It includes an overview of the main policies, regulations, initiatives, and stakeholders, as well as an outlook on future policies and initiatives that may impact the technologies of the EU Computing Continuum.
- Section **¡Error! No se encuentra el origen de la referencia.** presents the comprehensive strategy and the first result of its implementation, that has been developed to increase awareness of, and meaningful participation in, policy initiatives—particularly those led by the European Commission.
- Section **¡Error! No se encuentra el origen de la referencia.** builds upon the work presented in D3.1 [1], continuing the analysis of the role of Open Source as a key enabler of Digital Sovereignty for the EU Computing Continuum. In this section, the focus shifts to a case study in the agriculture sector, in contrast to the automotive sector examined in D3.1.
- Section 5 continues the in-depth analysis of the six key factors identified as critical for shaping EU technological sovereignty and the convergence of Edge, Cloud, and IoT technologies, by applying a SWOT analysis to each.
- Section 6 summarizes the main conclusions and key takeaways from the activities and events conducted in the international context, with a particular focus on engagement with Japanese stakeholders aiming to foster alignment and extract lessons learned at both the policy and technology prospection levels.
- The Conclusions section wraps up the report and foresees the future activities to be implemented in the context of policy and regulatory analysis.

## 2 Mapping European policy and regulatory landscape in the computing Continuum

### 2.1 The policy-technology matrix

NexusForum.EU has mapped the European policy and regulatory landscape in the Computing Continuum by selecting specific elements along the continuum and specific legal and policy instruments, to draw how the regulatory scene impacts the technological components as depicted in Figure 1 and Figure 2. This content has been written to be read by industrial stakeholders through the EUCEI [website](#) and is being continuously updated based on the monitoring of the policies and the evolution of the NexusForum.EU research and innovation roadmap.

Name of Policy/Act/Initiative	How is that technology impacted				
Establishing the European High Performance Computing Joint Undertaking					
An EU initiative on Web 4.0 and virtual worlds					
Cyber Solidarity Act					
eIDAS					
AI Act					
Data Governance Act					
Connecting Europe Facility					
Digital Decade Policy Programme 2030					
Establishing the European Electronic Communications Code					
Digital Services Act					
Digital Markets Act					
Chips Act					
Framework for the free flow of non-personal data in the European Union					
Data Act					
NIS 2					
Cybersecurity Act					
Cyber Resilience Act					
	AI for cloud-edge	Cloud-edge for AI	GenAI for infrastructure	Telco cloud-edge	Cloud-edge use cases
	Specific field in which the company is involved				

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

Name of Policy/Act/Initiative	How is that technology impacted					
Establishing the European High Performance Computing Joint Undertaking						
An EU initiative on Web 4.0 and virtual worlds						
Cyber Solidarity Act						
eIDAS						
AI Act						
Data Governance Act						
Connecting Europe Facility						
Digital Decade Policy Programme 2030						
Establishing the European Electronic Communications Code						
Digital Services Act						
Digital Markets Act						
Chips Act						
Framework for the free flow of non-personal data in the European Union						
Data Act						
NIS 2						
Cybersecurity Act						
Cyber Resilience Act						
	Carbon-neutral AI	Hardware level	Software development	Cybersecurity	Next gen AI	Data/data spaces
	Specific field in which the company is involved					

Figure 2. Excerpt 2 of the interactive policy matrix on the EUCloudEdgeIoT.eu website

This matrix clarifies how each legal or policy instrument impacts either a stakeholder wanting to use a specific Computing Continuum technology or how it impacts a stakeholder developing this kind of technology. The only exception to these criteria is cybersecurity, since it is not a type of technology but rather a transversal topic of the Research and Innovation roadmap. Furthermore, for each intersectional factor, the project provides an external website or external FAQ document for any question a user may have regarding the specific policy or legal tool analysed.

### 2.1.1 The impact of selected EU policy and legal instruments along the Computing Continuum

One of the main objectives of the policy and regulatory framework in NexusForum.EU is to provide policy recommendations that contribute to the convergence of cloud, edge and IoT technologies, through the integration and consolidation of the technologies prioritized in the NexusForum.EU Research and Innovation Roadmaps and promoting closer collaboration with the industry.

NexusForum.EU is identifying key technology priorities and needs for strengthening European competitiveness in cloud, edge and IoT technologies, and in particular in supporting the development of AI technologies in Europe. Additionally, the project is continuously providing up-to-date analyses of the relevant policy landscape and identifying gaps and opportunities concerning the identified technology priorities and needs. All these inputs are

necessary to define the analysis framework that we are proposing to use to develop the recommendations.

The following subsections discuss how specific EU policy and legal instruments impact a stakeholder either developing or using a Computing Continuum technology.

### *2.1.1.1 Establishing the European High Performance Computing Joint Undertaking*

- **Cloud-edge for AI:** This initiative enhances Europe's supercomputing capabilities, providing businesses with access to cutting-edge computing power for AI model development and data processing. It ensures compliance with EU data protection laws, offering AI companies secure, sovereign cloud-edge services. By reducing dependency on non-EU providers, the initiative boosts the competitiveness of European AI firms both locally and globally. It also promotes innovation through collaborative research and cost-effective access to high-performance resources. Due to its emphasis on sustainability, it enables businesses to run energy-efficient, large-scale AI applications while lowering operational costs. For more information, please visit: <https://op.europa.eu/en/web/who-is-who/organization/-/organization/corporate-body/EUROHPC>
- **Hardware level:** EuroHPC JU provides companies with access to advanced high-performance computing (HPC) resources enabling them to perform complex simulations, computational modelling, and data-intensive analytics more efficiently. This can drive innovation and enhance their competitiveness, being able to develop cutting-edge solutions, optimize production processes, and reduce time-to-market for new products. It also offers funding opportunities and support for SMEs to integrate HPC into their operations.  
In its projects, EuroHPC JU places a strong emphasis on sustainability and ethical issues. Businesses should conduct their operations in accordance with these guidelines to make sure that their efforts support the EU's overarching objectives of ethical innovation and sustainability (such as low-power micro-processing components). For additional details: Get in touch with [Contact - EuroHPC JU](#).

### *2.1.1.2 An EU initiative on Web 4.0 and virtual worlds*

- **Cloud-edge use cases:** The initiative aims to advance the next generation of the internet, creating immersive, decentralised environments that integrate AI, blockchain, and advanced cloud-edge computing. For businesses using or producing cloud-edge AI solutions, this offers new opportunities to leverage virtual worlds for innovative products, services and customer engagement. The initiative encourages collaboration between tech companies to develop scalable and secure virtual platforms, enhancing cross-sector use cases like e-commerce, healthcare and education. It also fosters data sovereignty and privacy by ensuring European regulations govern these virtual environments. y investing in Web 4.0, companies can access cutting-edge infrastructure and expand their capabilities in real-time, decentralised and interactive AI applications. For more information, please visit: [https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda\\_23\\_3719/QANDA\\_23\\_3719\\_EN.pdf](https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda_23_3719/QANDA_23_3719_EN.pdf)

### 2.1.1.3 Cyber Solidarity Act

- **Cybersecurity:** By establishing a pan-European infrastructure of Security Operations Centres (European Cyber Shield), the Act seeks to enhance real-time detection and situational awareness of cyber threats. This initiative mandates that European companies, especially those operating critical infrastructures, align their technologies with standardized detection and response protocols. Consequently, businesses are encouraged to adopt advanced cybersecurity measures and participate in information-sharing frameworks, thereby strengthening their resilience against cyber threats and contributing to a more secure digital ecosystem across the EU. For more information, you can ask your questions [here](#)<sup>1</sup>

### 2.1.1.4 EIDAS

- **Cybersecurity:** eIDAS Regulation establishes a comprehensive framework for electronic identification and trust services across the European Union. By standardizing electronic identification and authentication processes, it enhances the security of digital transactions for European companies. The regulation mandates rigorous requirements for electronic signatures, seals, and timestamps, ensuring data integrity and authenticity. Consequently, businesses are encouraged to adopt secure electronic identification systems and trust services, thereby strengthening their cybersecurity posture and facilitating trusted cross-border digital interactions. For more information, visit this page: <https://digital-strategy.ec.europa.eu/en/policies/learn-about-eidas>

### 2.1.1.5 AI Act

- **AI for cloud-edge, Cloud-edge for AI, Carbon neutral AI, NextGen AI and GenAI for infrastructure:** Depending on its risk classification level, the AI Act imposes specific obligations to which the company has to adhere. Furthermore, the data generated by the AI systems and data used to train AI models needs to respect transparency measures. For more information, you can submit your questions here: <https://aiacthub.eu/>
- **Software development:** The AI Act establishes strict regulations for AI systems in the EU, impacting software development by enforcing risk-based classification, with high-risk AI systems requiring compliance with risk assessments, data governance, and human oversight. Certain AI practices, like manipulative AI and social scoring, are banned, while transparency and accountability obligations require clear documentation and user disclosures. The Act also supports innovation through regulatory sandboxes for AI testing. Non-compliance can lead to fines of up to €35 million or 7% of global turnover, making adherence essential for AI developers operating in Europe. For more information, you can submit your questions here: <https://aiacthub.eu/>
- **Cybersecurity:** The Artificial Intelligence Act establishes harmonized rules for the development, placement on the market, and use of AI systems within the European Union.

---

<sup>1</sup> For more information, you can ask your questions here: [https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda\\_23\\_2244/qanda\\_23\\_2244\\_en.pdf](https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda_23_2244/qanda_23_2244_en.pdf)  
[https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda\\_23\\_2244/qanda\\_23\\_2244\\_en.pdf](https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda_23_2244/qanda_23_2244_en.pdf)



By categorizing AI applications based on risk levels, it mandates stringent security requirements for high-risk AI technologies, ensuring that European companies develop and deploy AI solutions that are secure and trustworthy. This regulatory framework compels businesses to implement robust cybersecurity measures, conduct thorough risk assessments, and ensure transparency in AI operations, thereby enhancing the overall security and trustworthiness of AI technologies used by European companies. For more information, you can submit your questions here: <https://aiacthub.eu/>

### 2.1.1.6 Data Governance Act

- **Data\Data Spaces:** The European regulation that aims to create a framework to facilitate European data spaces and increase trust between actors in the data market. The DGA entered into force in June 2022 and applies from Sept 2023. The DGA defines the European Data Innovation Board (EDIB). The Data Governance Act (DGA Article 30(h)) defines that the European Data Innovation Board will propose guidelines for common European data spaces. The guidelines shall address, among other things: (i) cross-sectoral standards for data sharing, (ii) counter barriers to market entry and avoiding lock-in effects and ensuring fair competition and interoperability, (iii) protection for lawful data transfers to third countries, (iv) non-discriminatory representation of relevant stakeholders in the governance of common European data spaces and (v) adherence to cybersecurity requirements. For more information, please visit: <https://eur-lex.europa.eu/eli/reg/2022/868/oj>

### 2.1.1.7 Connecting Europe Facility

- **Telco Cloud-Edge:** The Facility impacts telco cloud edge technologies by providing funding to support the deployment of high-performance digital infrastructure across Europe. Through the Facility, European firms developing this kind of technologies can access grants for projects that enhance connectivity, improve digital services, and expand broadband networks, particularly in underserved remote areas. For telco providers, the funding can help scale edge data centres and 5G infrastructure, fostering innovation in low-latency services. By improving the backbone for cloud-edge services, the Facility enables businesses to deliver faster, more reliable services to end-users. This creates opportunities for both providers and consumers, with European companies better positioned in the competitive global digital landscape. For more information, please visit: [https://hadea.ec.europa.eu/calls-tenders\\_en](https://hadea.ec.europa.eu/calls-tenders_en), or ask your questions here: [https://hadea.ec.europa.eu/contact-form\\_en](https://hadea.ec.europa.eu/contact-form_en)
- **Carbon Neutral AI:** The Regulation establishing the “Connecting Europe Facility” does not exclusively focus on the European digital ecosystem but rather looks at trans-European networks in the transport, energy and digital sectors. This means that, while virtually having the potential to touch upon all the roadmap technologies, it can be found to indirectly address Telco cloud-edge, integration with 5G and 6G and Carbon-neutral edge/AI, Carbon Neutral Edge Intelligence, considering in particular its energy- and environment-related objectives. The Regulation defines a key funding scheme which directly targets the digital ecosystem, making grant opportunities available for eligible initiatives. More information on calls for proposals: [https://hadea.ec.europa.eu/programmes/connecting-europe-facility\\_en](https://hadea.ec.europa.eu/programmes/connecting-europe-facility_en)



### 2.1.1.8 Digital Decade Policy Programme 2030

- AI for Cloud-Edge, Cloud-Edge for AI, Telco Cloud-Edge:** EU programme designed to promote innovation and investment in the EU. One of its main objectives is to support the development of comprehensive and sustainable ecosystem of interoperable digital infrastructures, where high performance, edge, cloud, quantum computing, artificial intelligence, data management and network connectivity converge. In concrete terms, the ambition is to reach at least a 75% of cloud computing services, big data or artificial intelligence uptake by European businesses. For more information, please visit: <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>
- Carbon Neutral AI:** According to Article 3.1 (e), The Decision aims at developing a comprehensive and sustainable ecosystem of interoperable digital infrastructures, where high performance, edge, cloud, quantum computing, artificial intelligence, data management and network connectivity work in convergence, to promote their uptake by businesses in the Union, and to create opportunities for growth and jobs through research, development and innovation, and ensuring that the Union has a competitive, secure and sustainable data cloud infrastructure in place, with high security and privacy standards and complying with the Union data protection rules. The scope of the Decision is quite wide-encompassing, and as such touches upon several of the technologies examined in the roadmap, with particular reference to AI for Cloud, Cloud for AI, Carbon-neutral edge/AI, Carbon Neutral Edge Intelligence, Cybersecurity and indirectly addresses Telco cloud-edge, integration with 5G and 6G and Hardware level (HPC – RISC-V). For more information, please visit: <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>
- Hardware level:** The Digital Decade Policy Programme 2030's goal is to transform Europe's digital landscape by setting ambitious targets for digital infrastructure; this includes widespread gigabit connectivity and advanced semiconductors, driving demand for efficient hardware solutions. It focuses on sustainable and secure digital infrastructures, requiring hardware manufacturers to comply with strict security regulations. For example, one of the digital goals is for the Union to produce at least 20% of the world's value of advanced semiconductors in compliance with Union law on environmental sustainability. The programme drives innovation through multi-country projects and highlights the need for digital skills across the workforce. In this context, SMEs play a crucial role, with goals for over 90% to achieve basic digital intensity and providing opportunities for funding and collaboration on innovative projects. For more information, please visit: <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>
- Cybersecurity:** The Digital Decade Policy Programme 2030 outlines the European Union's vision for digital transformation by 2030, emphasizing the importance of robust cybersecurity measures. It sets specific targets for digital skills, infrastructure, and public services, encouraging European companies to invest in secure digital infrastructures and adopt best practices to protect against cyber threats. By promoting the development of secure digital technologies and services, the programme aims to enhance the overall cybersecurity posture of businesses operating within the EU. For more information: <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>

### 2.1.1.9 Establishing the European Electronic Communications Code

- AI for cloud-edge:** The ECC promotes the rollout of faster, more reliable networks by encouraging investment in high-speed broadband and 5G. As it pushes for a better broadband connectivity across the EU, AI-powered applications in industries and it includes provisions around data privacy and sovereignty, like, for example, complying with GDPR and other EU regulations. For more information, please visit: [https://ec.europa.eu/commission/presscorner/detail/en/memo\\_18\\_4084](https://ec.europa.eu/commission/presscorner/detail/en/memo_18_4084)
- Cloud-Edge for AI:** The Code supports the enhancement of 5G networks and edge infrastructure, which helps companies develop AI applications that require low latency and high bandwidth. Since it pushes for infrastructure sharing, the code is very relevant for smaller firms looking to leverage AI without needing giant upfront investments in network infrastructure. It also encourages innovation through public-private partnerships, which could foster AI solutions that are more integrated with cloud-edge infrastructure. For more information, please visit: [https://ec.europa.eu/commission/presscorner/detail/en/memo\\_18\\_4084](https://ec.europa.eu/commission/presscorner/detail/en/memo_18_4084)
- Cloud-Edge use cases:** The Code directly impacts the development of network infrastructure, regulation, and service delivery models that are essential to edge computing. The Code promotes the rollout of high-speed broadband such as fiber-optic networks and next-generation technologies such as 5G, which are crucial for cloud-edge operations. Given the support to enhancing broadband infrastructure and accelerating 5G deployment, this EU instrument can be beneficial for use cases like autonomous vehicles, IoT (i.e. smart cities) and real-time data processing where latency is of critical importance. For more information, please visit: [https://ec.europa.eu/commission/presscorner/detail/en/memo\\_18\\_4084](https://ec.europa.eu/commission/presscorner/detail/en/memo_18_4084)
- Cybersecurity:** European Electronic Communications Code (EECC), establishes a comprehensive regulatory framework for electronic communications within the European Union. It emphasizes the security and integrity of public electronic communications networks and services. The directive mandates that providers implement appropriate technical and organizational measures to manage risks posed to the security of networks and services, ensuring a level of security appropriate to the risk presented. This includes measures to prevent and minimize the impact of security incidents on users and interconnected networks. By enforcing these requirements, the EECC enhances the cybersecurity posture of European companies operating in the electronic communications sector, ensuring the resilience and reliability of their services. Ask your questions here: [https://ec.europa.eu/commission/presscorner/detail/en/memo\\_18\\_4084](https://ec.europa.eu/commission/presscorner/detail/en/memo_18_4084)

### 2.1.1.10 Digital Services Act

- AI for Cloud-Edge:** For AI-driven cloud-edge solutions, companies must ensure their algorithms are transparent and free from bias, in particular when handling user data. The Act mandates that cloud-edge platforms using AI must take responsibility for harmful or illegal content, which requires robust monitoring and compliance mechanism. AI systems interacting with user-generated content must have mechanisms for content moderation. This mandates companies to implement safeguards to protect users' rights and privacy when deploying AI in edge computing environments. For more information, please visit: <https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers>

- **Cloud-Edge for AI:** The Act enforces strict rules around data protection and transparency when deploying AI in the edge, especially in user-sensitive applications. Due to these technologies' reliance on data storage across different locations, it is critical to comply with data sovereignty and content moderation standards. The Act also pushes cloud-edge providers to adopt more rigorous data governance and monitoring framework, since it holds companies accountable for the legal and ethical implications of AI-driven services with the aim of obtaining mechanisms that mitigate risks such as harmful algorithmic outputs or privacy violations. For more information, please visit: <https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers>
- **Software development:** The Digital Services Act (DSA) impacts software development by enforcing stricter content moderation, requiring platforms to detect and remove illegal content while ensuring transparency in moderation decisions. It also limits targeted advertising, particularly for minors and sensitive data, affecting ad-tech development. Algorithmic transparency is mandated, giving users more control over personalized content. Developers must also implement business user traceability for online marketplaces to verify seller identities, enhancing trust. These regulations push software companies to build more responsible, transparent, and secure digital services. Ask your questions here: <https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers>
- **Data/Data Spaces:** The Digital Services Act (DSA) is an EU regulation adopted in 2022 that addresses illegal content, transparent advertising and disinformation. It updates the Electronic Commerce Directive 2000 in EU law, and was proposed alongside the Digital Markets Act (DMA). The DSA, with its emphasis on consumer protection and due diligence, provides a framework that can adapt to evolving challenges in the digital realm. For more information, please visit: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>

### 2.1.1.11 *Digital Markets Act*

- **AI for Cloud-Edge:** The Digital Markets Act aims to ensure fair competition, prevent monopolistic practices, and foster innovation in digital markets. For companies developing AI for cloud-edge technology, the DMA might affect how they interact with dominant platforms, particularly if they rely on or integrate with gatekeeper services like cloud infrastructures, app stores, or search engines. It could limit practices that gatekeepers use to favour their own services over competitors, which might affect access to markets or data. For users, the Act ensures better access to more diverse services, lower prices, and more choices by curbing anti-competitive behaviours. For AI developers and users alike, the Act promotes a more level playing field and encourages innovation, ensuring smaller firms aren't stifled by the power of dominant market players. For more information, please visit: [https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers\\_en](https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers_en)
- **Cloud-Edge for AI:** If a company developing or using cloud-edge AI solutions is considered as a Gatekeeper under the Digital Markets Act affects, or else is designated as a large platform with significant control over access to users and services - such as major cloud providers or AI-driven platforms - some restrictions may apply. Indeed, these parties must comply with strict obligations to prevent anti-competitive practices, like self-preferencing and restricting third-party access to their services. The Act ensures that smaller companies, including AI startups, can access the same market opportunities, promoting innovation and fair competition. Violating the Digital Markets Act provisions could result in substantial fines, impacting both gatekeepers and users reliant on their services. For more information, please visit: [https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers\\_en](https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers_en)

[act.ec.europa.eu/about-dma/questions-and-answers\\_en](https://act.ec.europa.eu/about-dma/questions-and-answers_en)

- **Telco Cloud-Edge:** For European companies developing telco cloud-edge solutions, the Digital Markets Act could impose stricter rules on gatekeeper platforms, fostering a more level playing field and encouraging innovation. It aims at the prevention of market dominance by few players, allowing smaller firms in the telecom sector to compete more efficiently. Users of these technologies may benefit from more competitive pricing and improved service offering as a result of increased market fairness. For more information, please visit: [https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers\\_en](https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers_en)
- **Cloud-Edge use cases:** For cloud-edge use cases, the Digital Markets Act implies that smaller Eu companies developing new services are less likely to face unfair advantages from dominant platform providers. The act helps create a more level playing field, fostering innovation by allowing emerging players to compete on more equal terms. Companies in sectors like fintech, retail, or media can particularly benefit as the act ensures they have the opportunity to scale up their cloud-edge solutions without being stifled by market concentration. For more information, please visit: [https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers\\_en](https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers_en)
- **Software development:** The Digital Markets Act (DMA) ensures fair competition in the EU digital sector by imposing obligations on gatekeepers—large tech companies controlling key digital services. It mandates interoperability, allowing third-party developers to integrate with dominant platforms, and prohibits self-preferencing, ensuring fair treatment of competing services. The DMA also enforces data portability, requiring platforms to enable users to transfer their data, and access to platform data, allowing businesses to leverage user-generated data for innovation. These measures create a more competitive and transparent software development landscape. For more information, you can ask your questions here: [https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers\\_en](https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers_en)
- **Cybersecurity:** The Digital Markets Act aims to ensure fair and contestable markets in the digital sector by imposing obligations on designated "gatekeeper" platforms. While its primary focus is on promoting competition, the regulation indirectly impacts cybersecurity by requiring these gatekeepers to implement measures that prevent unauthorized access and ensure the integrity of their services. This includes obligations to allow interoperability with third-party services in a secure manner and to provide users with effective control over their data. Consequently, European companies interacting with these platforms can expect enhanced security measures, reducing potential vulnerabilities and contributing to a safer digital ecosystem. For more information, you can ask your questions here: [https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers\\_en](https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers_en)
- **Next gen AI:** The digital Markets Act is aimed at guaranteeing a competitive and fair digital sector. The act lays out provisions to help smaller providers of digital services operate in the digital market. The act sets out to achieve this by defining obligations for 'gatekeepers' (i.e., particularly large service providers, as defined in Article 3) to reduce the obstacles posed to other actors attempting to access the market. Summary of the main points of the act: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legisum:4622237>

### 2.1.1.12 Chips Act

- Telco Cloud-Edge:** Companies developing telco cloud-edge solutions are impacted by the Chips Act in terms of funding and incentives to build and scale semiconductor manufacturing within Europe, which in return enhances supply chain for critical hardware. This can lead to more reliable and cost-effective components for telco infrastructures. Users of cloud-edge technologies can benefit from improved hardware availability, performance and security, as European-made advanced chips are prioritized. For more information, please visit: [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_23\\_4519](https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_4519)
- Cloud-edge use cases:** The Chips Act is significant for cloud and edge computing as it directly impacts the hardware on which these services are built. Indeed, the Act focuses on increasing semiconductor production within the EU and ensuring access to cutting-edge chips. By supporting local chip manufacturing, the act can reduce supply chain dependencies and boost innovation in specialised processing power required for edge computing. Companies developing use cases in AI, autonomous vehicles, supercomputing, defence and space capabilities or smart cities can particularly benefit from this, as localised access to high performance chips can lead to faster, more efficient edge-based computations. For more information, please visit: [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_23\\_4519](https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_4519)
- Hardware level:** The European Chips Act has several key goals aimed at strengthening Europe's position in the semiconductor industry; some of these are: increasing production capacity to 20% of the global market by 2030, enhancing innovation in chip design and manufacturing, ensuring supply chain resilience, and supporting start-ups and SMEs through improved financing access. The Act introduces measures to streamline the process and fast-track procedures for semiconductor manufacturing facilities, helping companies to bring new technologies to market faster. On the other hand, the creation of a European Chips Infrastructure Consortium encourages collaboration between public and private sectors, fostering innovation and technological advancement. You can find more information here: [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_23\\_4519](https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_4519)

### 2.1.1.13 Framework for the free flow of non-personal data in the European Union

- Cloud edge for AI:** This Regulation aims to eliminate data localization requirements within the EU, promoting the free movement of non-personal data across member states. This framework is particularly relevant for companies developing or using cloud-edge AI technologies, as it enables them to store, process, and transfer non-personal data freely across borders within the EU. By removing restrictions on where non-personal data can be stored or processed, it supports innovation and efficiency, helping businesses scale and enhance their AI solutions. However, companies must still comply with EU data protection laws like the GDPR for personal data, ensuring that data privacy and security standards are maintained. This regulation thus facilitates more seamless data flows, while balancing the need for security and compliance. For more information, please visit: <https://digital-strategy.ec.europa.eu/en/faqs/business-government-data-sharing-questions-and-answers>



- **Telco Cloud-Edge:** Companies developing telco cloud-edge solutions are impacted by the Chips Act in terms of funding and incentives to build and scale semiconductor manufacturing within Europe, which in return enhances supply chain for critical hardware. This can lead to more reliable and cost-effective components for telco infrastructures. Users of cloud-edge technologies can benefit from improved hardware availability, performance and security, as European-made advanced chips are prioritized. For more information, please visit: [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_23\\_451](https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_451)
- **Cybersecurity:** This Regulation establishes a framework for the free flow of non-personal data within the European Union. By prohibiting data localization requirements, except when justified on grounds of public security, it enables European companies to store and process non-personal data across borders, enhancing operational flexibility and efficiency. The regulation encourages the development of self-regulatory codes of conduct to facilitate data portability and minimize vendor lock-in, promoting a competitive and secure data economy. This approach ensures that businesses can implement robust cybersecurity measures consistently across the EU, fostering a more resilient digital environment. For more information, you can ask you questions here: <https://digital-strategy.ec.europa.eu/en/faqs/business-government-data-sharing-questions-and-answers>
- **Data/Data Spaces:** This regulation aims at removing obstacles to the free movement of non-personal data between different EU member states and IT Systems in Europe. It ensures that every organisation should be able to store and process data anywhere in the EU; the data is available for regulatory control by public authorities; Easier switching between cloud service providers for professional users; Full consistency and synergies with the cybersecurity package. For more information, please visit: <https://eur-lex.europa.eu/eli/reg/2018/1807/oj>

#### 2.1.1.14 Data Act

- **AI for Cloud-Edge:** The EU Data Act aims to improve the accessibility and sharing of data across the EU, enhancing the use of data for innovation while ensuring security and privacy. For companies developing AI for cloud-edge technology, the Data Act mandates that they make certain data generated by their products accessible to third parties under clear conditions, fostering data sharing and interoperability. This could help fuel innovation in AI by making data more available for training and improving algorithms. For users, the Data Act offers greater control over their data, ensuring they can access, share, and even transfer their data across platforms. However, the law also includes provisions to ensure that such data sharing doesn't compromise privacy or security, aligning with broader EU data protection regulations. For more information, please visit: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act>
- **Cloud-Edge for AI:** The Data Act is designed to regulate the access, sharing, and use of data across the European Union, particularly focusing on enhancing data portability, availability, and use for innovation. For companies dealing with the development of cloud-edge AI solutions, the Act impacts how data generated or processed by their products can be accessed and shared with third parties. It mandates that data generated by IoT devices, AI systems, and other digital technologies be made accessible to users and businesses, subject to clear terms and conditions, while safeguarding privacy and security. This could influence how AI providers structure their services and data-sharing

agreements, ensuring compliance with the rules on data ownership, consent, and transfer. Additionally, it creates a more open data environment, potentially boosting innovation but also requiring strict adherence to data protection standards. For more information, please visit: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act>

- GenAI for infrastructure:** The Data Act is a far-reaching Regulation which covers the wider European data ecosystem, regulating the exchanges of data as well of the protection and exchange of data in specific contexts. The regulation requires actors in the digital ecosystem to make certain types of data available for third parties, thus contributing to the data economy and reducing the barriers for consumers to switch between different data processing services. The regulation also outlines provisions for the protection of trade secrets and does not reduce the scope of application of the General Data Protection Regulation. Given its cross-cutting domain of application, the Data Act is of relevance to AI implementations managing and generating data and the exchange of data. For more information, please visit: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act>
- Telco Cloud-Edge:** The Data Act could amplify data sharing across borders and sectors, creating new opportunities for innovation and service offerings. This would benefit companies developing telco cloud-edge solutions, while also increasing the level of transparency of data usage, which could help smaller market players compete with larger players. On the other hand, users of these technologies would likely experience more accessible, secure, and fair data practices, enhancing trust in services, and granting them more freedom of choice when it comes to data storage. For more information, please visit: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act>
- Cloud-Edge use cases:** The Data Act influences cloud-edge uses cases put forward by third parties because it aims at ensuring interoperability between different platforms and services. It also encourages innovation by promoting the use of data across borders, driving new business models. Firms developing solutions for industries such as IoT, agriculture, or manufacturing stand to benefit as the Act encourages the flow of real-time data for edge analytics and decision-making. For more information, please visit: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act>

### 2.1.1.15 NIS2

- Cybersecurity:** The NIS2 Directive establishes a unified legal framework to uphold cybersecurity across 18 critical sectors within the European Union. It mandates that both "essential" and "important" entities implement appropriate technical and organizational measures to manage cybersecurity risks, conduct regular risk assessments, and report significant incidents to relevant authorities. The directive also emphasizes the accountability of management bodies, introducing potential personal liability for non-compliance. By enforcing these requirements, the NIS2 Directive enhances the cybersecurity posture of European companies, ensuring the resilience and reliability of their services. For more information: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

### 2.1.1.16 Cybersecurity Act

- AI for Cloud-Edge:** The Act enhances the mandate of the European Union Agency for Cybersecurity (ENISA). For companies developing AI for cloud-edge technology, the act mandates that certain critical digital products and services must meet specific cybersecurity standards, ensuring that they are resilient to cyber threats. This also involves a new certification system, which can help companies demonstrate compliance with cybersecurity best practices and build trust in their products. For users, the Cybersecurity Act offers greater assurance that the AI and digital products they use are secure, reducing the risk of cyberattacks. It enhances transparency by requiring companies to disclose their security practices and ensuring that the EU has more centralized and effective cybersecurity governance. For more information, please visit:
- Cloud-edge for AI:** The EU Cybersecurity Act strengthens the EU's overall cybersecurity framework. It establishes the European Cybersecurity Certification Framework, which sets standards for cybersecurity certification across various sectors, including AI and cloud-edge technologies. Companies developing or using AI technology solutions within the EU are impacted by the Act, as they may be required to obtain cybersecurity certifications for their products and services. This ensures that these solutions meet high cybersecurity standards, mitigating risks for users and increasing trust in the technologies. Non-compliance could result in market restrictions and reduced competitiveness in the EU. For more information, please visit: [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_19\\_3369](https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_3369)
- GenAI for infrastructure:** On top of strengthening the EU Agency for cybersecurity (ENISA), the EU Cybersecurity Act “introduces an EU-wide cybersecurity certification framework for ICT products, services and processes”, this means that the measures defined in the act are cross-cutting and apply on a wide range of digital goods and services. Cybersecurity measures outlined in the Act may apply to some implementations of Generative AI for infrastructure. For more Information and updates on the Cybersecurity Certification, please visit: [https://certification.enisa.europa.eu/index\\_en](https://certification.enisa.europa.eu/index_en)
- Telco cloud-edge:** The Act strengthens the EU's cybersecurity framework, setting clear cybersecurity standards that companies developing telco cloud-edge solutions must meet, ensuring greater security and trust in their offerings. The Act also mandates that critical infrastructure, including telecom networks, implement robust cybersecurity measures, which could drive higher compliance costs but also offer opportunities to differentiate through secure services. Users of these technologies benefit from improved protection against cyber threats and greater confidence in the reliability of services. For more information, please visit: [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_19\\_3369](https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_3369)
- Cloud-edge use cases:** The Cybersecurity Act establishes requirements for cybersecurity certification, which directly impacts cloud and edge computing use cases, especially for EU-based companies. Cloud and edge providers offering services within the EU must adhere to robust security standards, ensuring that their infrastructures are resilient against cyber threats. This is relevant for industries like healthcare, finance, and critical infrastructure that require high levels of trust and data protection. Companies offering such solutions benefit from the Act by gaining trust in the marketplace through recognized certifications, which enhances their appeal to EU consumers who prioritise security and compliance. For more information, please visit:



[https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_19\\_3369](https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_3369)

- **Carbon Neutral AI:** On top of strengthening the EU Agency for cybersecurity (ENISA), the EU Cybersecurity Act “introduces an EU-wide cybersecurity certification framework for ICT products, services and processes”, this means that the measures defined in the act are cross-cutting and apply on a wide range of digital goods and services. Cybersecurity measures outlined in the Act may apply to some Artificial Intelligence implementations.
- **Hardware level:** The European Cybersecurity Act mainly focuses on establishing a framework for cybersecurity certification of ICT products, services, and processes. This framework will enable the assurance that hardware products meet specific security standards, at different levels depending on the risk of its use. The compliance with this certification will facilitate the access to the European Market as well as gain the consumers’ trust. Furthermore, the act aims to achieve a consistent approach to cybersecurity for hardware products. For further details visit European Chips Act - Questions and Answers or contact ENISA [info@enisa.europa.eu](mailto:info@enisa.europa.eu)
- **Software development:** The Cybersecurity Act establishes an EU-wide cybersecurity certification framework, requiring software developers to align with standardized security measures. It defines three assurance levels (basic, substantial, high), pushing developers to implement appropriate security measures. The Act promotes security by design and default, ensuring software is secure from the outset, and mandates vulnerability handling and disclosure, requiring continuous monitoring, patching, and transparency in security updates. For more information, you can ask your questions here: [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_19\\_3369](https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_3369)
- **Cybersecurity:** The Cybersecurity Act enhances the role of the European Union Agency for Cybersecurity (ENISA) and establishes a comprehensive framework for cybersecurity certification of information and communications technology (ICT) products, services, and processes. By providing a standardized approach to cybersecurity certification, the Act aims to increase trust and security in digital products and services across the EU. European companies benefit from clear guidelines and certification schemes, enabling them to demonstrate the cybersecurity robustness of their offerings, thereby enhancing their competitiveness and ensuring compliance with EU-wide security standards. For more information, you can ask your questions here: [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_19\\_3369](https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_3369)
- **Next Gen AI:** On top of strengthening the EU Agency for cybersecurity (ENISA), the EU Cybersecurity Act “introduces an EU-wide cybersecurity certification framework for ICT products, services and processes”, this means that the measures defined in the act are cross-cutting and apply on a wide range of digital goods and services. Cybersecurity measures outlined in the Act may apply to some Artificial Intelligence implementations. For more Information and updates on the Cybersecurity Certification, please visit: : [https://certification.enisa.europa.eu/index\\_en](https://certification.enisa.europa.eu/index_en)
- **Data \ Data Spaces:** Overall, the Cybersecurity Act aims to create a more secure and trustworthy digital environment, which has a direct impact on how data and data spaces technologies are developed, implemented, and maintained. The act establishes a framework for cybersecurity certification of ICT products, services, and processes. This means that data and data spaces technologies must adhere to higher security standards, ensuring better protection against cyber threats. This includes compliance to the proposed certification schemes (i.e., EUCS) and incorporation of robust risk management

practices among others. For more Information and updates on the Cybersecurity Certification, please visit: : [https://certification.enisa.europa.eu/index\\_en](https://certification.enisa.europa.eu/index_en)

### 2.1.1.17 *Cyber Resilience Act*

- **AI for Cloud-Edge:** The Cyber Resilience Act impacts companies developing AI products because it mandates that they integrate robust security measures into their design, ensuring resilience against cyber threats throughout the lifecycle of the product. This includes conducting risk assessments, implementing secure coding practices, and providing clear vulnerability management. For users, the Act offers a higher level of confidence in the security of cloud-edge AI products, as they will be subject to rigorous compliance standards, reducing exposure to cyber risks. In essence, it elevated the security bar for both product creators and end-users across the EU. For more information, please visit: [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_22\\_5375](https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5375)
- **Cloud-Edge for AI:** The EU Cyber Resilience Act imposes conditions on European companies developing or using AI for Cloud Edge technologies. Indeed, they must ensure that their products meet specific security requirements, such as secure development practices, timely updates, and risk management processes. Non-compliance could lead to penalties or restrictions in the EU market. Additionally, the act mandates that users and organizations using these technologies must adhere to safety protocols, ensuring robust protection against cyber threats. In practice, this drives both innovation and accountability in the security of AI and cloud-edge solutions. For more information, please visit:
- **GenAI for infrastructure:** The Cyber Resilience Act refers to products with digital elements entering the market, and aims to ensure the cybersecurity of all components within the supply chain. The specific requirements vary depending on the classification of the product, with particular reference to the level of risk. This is particularly relevant in the field of Generative AI for infrastructure, as AI components may be considered high-risk (Art. 12), and are therefore subject to specific requirements. For more information, please visit:  
<https://www.pwc.ch/en/insights/regulation/understanding-the-eu-cyber-resilience-act.html>
- **Hardware level:** The European Cyber Resilience Act (CRA) has a significant impact at hardware level as it sets mandatory cybersecurity standards for products with digital elements sold in the EU. It looks out for products to be secure throughout their lifecycle. Manufacturers must conduct conformity assessments to ensure their products meet the CRA's standards and are also required to report any actively exploited vulnerabilities to the European Union Agency for Cybersecurity (ENISA). For more information: Cyber Resilience Act - Questions and Answers or contact ENISA [info@enisa.europa.eu](mailto:info@enisa.europa.eu)
- **Software development:** The Cyber Resilience Act (CRA) enforces strict cybersecurity requirements for digital products in the EU, directly impacting software development. Developers must implement state-of-the-art security measures, ensure vulnerability management and timely updates, and comply with conformity assessments to obtain CE marking for market access. The Act also mandates transparent documentation of security measures for regulatory and consumer access. Non-compliance risks fines and market restrictions, making cybersecurity a critical aspect of software development for the EU market. For more information: Cyber Resilience Act - Questions and Answers or contact ENISA [info@enisa.europa.eu](mailto:info@enisa.europa.eu)

- **Cybersecurity:** The Cyber Resilience Act establishes comprehensive cybersecurity requirements for products with digital elements within the European Union. It mandates that manufacturers design, develop, and maintain these products with robust cybersecurity measures throughout their lifecycle. This includes ensuring protection against unauthorized access, reducing vulnerabilities, and providing security updates. By enforcing these standards, the Act enhances the cybersecurity posture of European companies, ensuring that digital products are resilient against cyber threats and fostering trust among consumers. For more information: Cyber Resilience Act - Questions and Answers or contact ENISA [info@enisa.europa.eu](mailto:info@enisa.europa.eu)
- **NextGen AI:** The Cyber Resilience Act refers to products with digital elements entering the market, and aims to ensure the cybersecurity of all components within the supply chain. The specific requirements vary depending on the classification of the product. This is potentially very relevant for Next gen AI, as products using future evolutions of the technology may be classified as 'high-risk' depending on their field of application. <https://www.pwc.ch/en/insights/regulation/understanding-the-eu-cyber-resilience-act.html>

## 2.2 Initiatives and Stakeholders

In NexusForum.EU, initiatives and stakeholders are considered across all project activities. To fully understand the policy landscape and the most recent regulatory developments, it is essential to take into account both public and private initiatives that are relevant and impactful. This helps the community better grasp various policy proposals, regulatory suggestions, and strategic decisions. As a result, relevant initiatives are included in the "Policies & Governance" section of the EUCEI platform and are regularly updated based on the outcomes and activities of other project tasks, particularly those related to stakeholder engagement and community building<sup>2</sup>. The current initiatives available to stakeholders for a deeper understanding of the Cloud Continuum ecosystem are presented in Figure 3.

<sup>2</sup> For further information please check [https://eucloudedgeiot.eu/wp-content/uploads/2024/08/D4.1\\_Engagement\\_and\\_Community\\_Report.pdf](https://eucloudedgeiot.eu/wp-content/uploads/2024/08/D4.1_Engagement_and_Community_Report.pdf)

[https://eucloudedgeiot.eu/wp-content/uploads/2024/08/D4.1\\_Engagement\\_and\\_Community\\_Report.pdf](https://eucloudedgeiot.eu/wp-content/uploads/2024/08/D4.1_Engagement_and_Community_Report.pdf)














 <b>Data Spaces Support Centre (DSSC)</b>	 <b>Simpl Programme</b>	 <b>SNS-JU, Smart Networks and Services</b>	 <b>Edge Observatory for the Digital Decade</b>
 <b>IPCEI CIS</b>	 <b>DOME Marketplace</b>	 <b>European Alliance for Industrial Data, Edge and Cloud</b>	 <b>AIOTI: Alliance for IoT and Edge Computing Innovation</b>
 <b>GAIA-X: A Federated Secure Data Infrastructure</b>	 <b>HIPEAC: Bridging industry and academia in computing systems</b>	 <b>NESSI: Networked European Services and Software Initiative</b>	 <b>BDVA: Big Data Value Association</b>
 <b>SovereignEDGE.EU: European Open Source for Europe's Next-Gen Edge Cloud</b>			

Figure 3. Initiatives collected in EUCEI web page.

## 2.3 Future Outlook

### 2.3.1 Upcoming EU policies meant to shape technology

This subsection provides an overview of recently released and upcoming policy documents aimed at shaping the EU technology ecosystem.

With the inception of the new 2024-2029 Commission and following the release of the report 'A competitiveness strategy for Europe' (Draghi Report),<sup>3</sup> the priorities of the European Commission have been aligned to respond to new and evolving challenges. This brought to the definition of a far-reaching policy roadmap for the coming months and years. The technological landscape of the European Union is mostly addressed in the Commission Priority 'A new plan for Europe's sustainable prosperity and competitiveness.'<sup>4</sup>

The main document outlining the upcoming policy actions planned, is the Commission Work Programme 2025<sup>5</sup>, which will be used in this paragraph to showcase both recently published policy documents and upcoming strategies and legislation.

The first Annex of the Commission Work Programme 2025<sup>6</sup> provides a comprehensive list of the planned policy actions to address the Commission Priority 'A new plan for Europe's sustainable prosperity and competitiveness', an excerpt of the annex is provided in the table below. As mentioned above, the table provides an overview of the planned policy action at EU level, categorising them based on their domain (column 2 of the table 1).

<sup>3</sup> Online, accessed on 22/04/2025: [https://commission.europa.eu/topics/eu-competitiveness/draghi-report\\_en](https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en)

<sup>4</sup> [https://commission.europa.eu/priorities-2024-2029/competitiveness\\_en](https://commission.europa.eu/priorities-2024-2029/competitiveness_en)

<sup>5</sup> COM(2025)45 final - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0045>

<sup>6</sup> COM(2025)45 final - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0045>

Table 1. Upcoming EU policies, as outlined in the Commission Work Programme 2025 [3]

Domain	Policy action
Competitiveness	Competitiveness Compass (non-legislative, Q1 2025)
Competitiveness	Single Market Strategy (non-legislative, Q2 2025)
Simplification	First Omnibus package on sustainability (legislative, Q1 2025)
Simplification	Second Omnibus package on investment simplification (legislative, Q1 2025)
Simplification	Third Omnibus package, including on small mid-caps and removal of paper requirements (legislative, Q2 2025)
Simplification	Revision of the Sustainable Finance Disclosure Regulation (legislative, incl. impact assessment, Article 114 TFEU, Q4 2025)
Simplification	Digital package (legislative, incl. impact assessment, Q4 2025)
Simplification	European Business Wallet (legislative, incl. impact assessment, Article 114 TFEU, Q4 2025)
Competitiveness and Decarbonisation	Clean Industrial Deal (non-legislative, Q1 2025)
Competitiveness and Decarbonisation	Action plan on affordable energy (non-legislative, Q1 2025)
Competitiveness and Decarbonisation	Industrial Decarbonisation Accelerator Act (legislative, incl. impact assessment, Article 114 TFEU, Q4 2025)
Competitiveness and Decarbonisation	EU Start-up and Scale-up Strategy (non-legislative, Q2 2025)
Competitiveness	Communication on a Savings and Investments Union (non-legislative, Q1 2025)
	Review of the Securitisation Framework (legislative, incl. impact assessment, Article 114 TFEU, Q2 2025)
Innovation	Digital Networks Act (legislative, incl. impact assessment, Article 114 TFEU, Q4 2025)
Innovation	AI Continent Action Plan (non-legislative, Q1 2025)
Innovation	Quantum Strategy of EU (non-legislative, Q2 2025)
Competitiveness	EU Space Act (legislative, incl. impact assessment, Article 114 TFEU, Q2 2025)
Competitiveness and Decarbonisation	Bioeconomy Strategy (non-legislative or legislative, Q4 2025)
Simplification	Targeted revision of the REACH Regulation (legislative, Article 114 TFEU, Q4 2025)
Security	Roadmap towards ending Russian energy imports (non-legislative, Q1 2025)
Competitiveness and Decarbonisation	Sustainable Transport Investment Plan (non-legislative, Q3 2025)



## A Competitiveness Compass for the EU (published January 2025)

The Competitiveness Compass<sup>7</sup> lays ground for the upcoming policies and strategies targeting both competitiveness and innovation objectives, in the context of a wider simplification of the policy framework and supporting technological innovation and streamlining the European research ecosystem.

The Communication ‘A Competitiveness Compass for the EU’ defines three flagship action pillars, respectively addressing three priority actions, namely *Closing the innovation gap*, *A joint roadmap for decarbonisation and competitiveness* and *Reducing excessive dependencies and increasing security*.

Several of the policy actions defined in Pillar 1 directly address the European digital ecosystem, namely:

- Start-up and Scale-up Strategy [Q2 2025]
- European Innovation Act [Q4 2025 – Q1 2026]
- AI Factories Initiative [Q1 2025]
- Apply AI, AI in Science, and Data Union Strategies [Q3 2025]
- EU Cloud and AI Development Act [Q4 2025 – Q1 2026]
- EU Quantum Strategy [Q2 2025] and a Quantum Act [Q4 2025]
- Digital Networks Act [Q4 2025]

The second and third pillars focus on aspects which are not specific to the digital ecosystem, while still providing wider orientations on sustainability, competitiveness and security which will have an impact on the Cloud, Edge and IoT sectors. In particular, Flagship Action Pillar 2 defines actions which the European digital ecosystem will be able to directly contribute to, for instance:

- Clean Industrial Deal and an Action Plan on Affordable Energy [Q1 2025]
- Industrial Decarbonisation Accelerator Act [Q4 2025]
- Strategic dialogue on the future of the European automotive industry and Industrial Action Plan [Q1 2025]
- Sustainable Transport Investment Plan [Q3 2025]
- Circular Economy Act [Q4 2026]

The actions listed above will likely steer innovations in the Cloud, Edge and IoT ecosystem towards sustainability objectives, for instance the implementation of IoT technologies to support environmental sustainability and energy efficiency in the manufacturing sector, in the automotive industry and in transport. Additionally, there is a clear link between circular economy and the reuse and repurposing of technological devices to extend their lifespan on the one side and increase the recovery of their components.

### 2.3.1.1 Recently published Communications

#### The Union of Skills (published March 2025)

In line with the competitiveness objectives outlined in the European Commission’s priority ‘A new plan for Europe’s sustainable prosperity and competitiveness’, the Commission

<sup>7</sup> COM(2025) 30 final – online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0030>

Communication ‘The Union of skills’,<sup>8</sup> seeks to respond to the need to improve the availability and retention of talents in key sectors for the European Union as well as to matching skills available and needed in the European market.

The Communication sets out to address this by defining four key objectives:

- ensure that everyone in Europe, no matter where they are, is empowered to build solid skills foundations and engage in lifelong upskilling and reskilling
- Upskill and reskill to ensure future-oriented skills
- Circulate and allocate skills to unlock the full potential of the single market
- Attract and retain skills from third countries to address skills shortages and develop top talent in Europe

With a view to address the objectives defined, the Communication outlines three key strand of activities, also defining a set of key deliverables at EU, national and regional level for each of the strands:

### *1. Building skills for life through a solid educational foundation*

Key deliverables:

- Action Plan on Basic Skills [Q1 2025]
- Basic Skills Support Scheme (pilot) [2026]
- 2030 Roadmap on the future of digital education and skills [Q4 2025]
- AI in education initiative [2026]
- STEM Education Strategic Plan [Q1 2025]
- EU Teachers and Trainers Agenda [2026]
- European competence framework for academic staff [2026]
- European Strategy for vocational education and training (VET) [2026]
- Increasing accessibility of higher education [2027]
- Intergenerational fairness strategy [Q1 2026]

### *2. Upskill and reskill to ensure future-oriented skills*

Key deliverables:

- Pilot a Skills Guarantee for workers [2025]
- Roll-out of targeted EU Skills Academies, after a review of existing ones [2026]
- Pilot transnational university-business partnerships for sectors with severe skills gaps [2026]

### *3. Circulate skills with the free movement of people across the EU, unlocking the single market's full potential*

- Skills Portability Initiative [2026]
- Common European framework for the automatic recognition of study qualifications and learning periods abroad in school, VET and higher education [2027]
- Launch of innovative joint European study programmes with a European degree/label [2026]
- A legal status for European Universities alliances [2027]
- Pilot a European VET diploma [2025-2026]

<sup>8</sup> COM(2025) 90 final - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0090>

- Pilot European School Alliances [2026]

#### 4. Attract, develop and retain talent

- Launch of the EU Talent Pool IT Platform
- Marie Skłodowska-Curie Action 'MSCA Choose Europe' Pilot [Q4 2025]
- A new Visa Strategy [Q4 2025]
- Launch of Multipurpose Legal Gateway Offices [2026]

Additionally, the Communication states the need to encourage funding beyond the EU's institutional budget, both from private and public entities to encourage the development and retention of talents in the EU.

Finally, yet importantly, the Communication defines ongoing and planned actions supporting governance on skills. These include internal and external cooperation actions to improve the availability and quality of data on skills, the establishment of a European Skills High Level Board and the potential development of a Recommendation on human capital.<sup>9</sup>

#### AI Continent Action Plan (published April 2025)

The flagship Communication 'AI Continent Action Plan'<sup>10</sup> specifically investigates the potential of Artificial Intelligence and outlines specific objectives to improve the European Union's competitiveness in the sector. The Plan provides key guiding principles to support the development, evolution and integration of Artificial Intelligence in the wider European market and digital ecosystem. The Communication revolves around five pillars, and their respective sub-pillars:

- Build large-scale AI data and computing infrastructures across Europe for the AI ecosystem
  - Deploy and scale AI Factories
  - Invest in AI Gigafactories
  - Establish the support framework for boosting EU cloud and data centre capacity
- Data for AI
- Foster innovation and accelerate AI adoption in strategic EU sectors
  - A use-case based approach in key European industry sectors and the public sector
  - European Digital Innovation Hubs as the key drivers for advancing AI deployment
  - AI "made in Europe" from research to the market
- Strengthen AI skills and talent
  - Enlarging the EU's pool of AI specialists
  - Upskilling and reskilling the EU workforce and population
- Fostering regulatory compliance and simplification

In the context of the AI Continent Action Plan and in line with the political priorities of the Competitiveness Compass, the European Commission has also launched the InvestAI

<sup>9</sup> Chapter 5. Governance, COM(2025) 90 final - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0090>

<sup>10</sup> COM(2025) 165 final - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2025:165:FIN>



initiative aimed at mobilising EUR 200 billion in public and private funds to support the European AI ecosystem, with particular reference to AI Gigafactories.

### **2.3.1.2 Upcoming policy actions**

#### **EU Quantum Strategy (Q2 2025) and Quantum Act (Q4 2025)**

According to the Communication ‘A competitiveness compass for the EU’, the EU Quantum Strategy<sup>11</sup> and the Quantum Act ‘will build on the existing Chips Act to address regulatory fragmentation, align EU and national programmes and support investment in pan-European quantum computing, communication and sensing infrastructure’<sup>12</sup>. The Quantum Strategy is planned for Q2 2025, and the Quantum Act is expected to follow, in Q4 2025.

#### **EU Start-up and Scale-up Strategy (Q2/Q3 2025)**

The EU Start-up and Scale-up Strategy, currently planned for Q2/Q3 2025 aims to ‘improve and simplify framework conditions for start-ups and scale-ups’<sup>13</sup>. The European Commission has launched a call for evidence to collect feedback on the key elements which will make up the upcoming Strategy. This phase concluded in March 2025. The call for evidence identified five critical areas of intervention to improve with a view to empower European start-ups, which will inform the drafting process for the Strategy, namely: i) limited access to finance, ii) regulatory and bureaucratic burden, iii) difficulty in accessing EU markets, iv) challenges in accessing talents and v) limited access to research and technology infrastructure, knowledge and support services.<sup>14</sup>

#### **Digital package (Q4 2025)**

The Digital Package<sup>15</sup> aims to simplify the Cybersecurity Act and more generally the EU’s cybersecurity framework. This is specifically addressing SMEs, with an aim to simplify their operation, market access, innovative capacity and competitiveness.

The Commission Communication ‘A simpler and faster Europe’<sup>16</sup> shares the simplification objectives outlined in the Digital Package. In particular, chapter III of the Communication, ‘Making Europe simpler and faster’, identifies a set of tools and actions to address the targets defined, namely a) new targets to reduce the administrative burden, b) prioritising new simplification measures, c) gradual stress-testing of the body of EU legislation d) a simpler, more focused and more impactful EU budget, and e) hands-on experience by conducting reality checks.

<sup>11</sup> <https://www.europarl.europa.eu/legislative-train/theme-a-new-plan-for-europe-s-sustainable-prosperity-and-competitiveness/file-eu-quantum-strategy>

<sup>12</sup> Chapter on ‘Excelling in the technologies for tomorrow’s economy’ - COM(2025) 30 final - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0030>

<sup>13</sup> Online, accessed on 23/04/2025 - [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14530-EU-Start-up-and-Scale-up-Strategy\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14530-EU-Start-up-and-Scale-up-Strategy_en)

<sup>14</sup> [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=intcom:Ares\(2025\)1232781](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=intcom:Ares(2025)1232781)

<sup>15</sup> <https://www.europarl.europa.eu/legislative-train/theme-a-new-plan-for-europe-s-sustainable-prosperity-and-competitiveness/file-digital-package>

<sup>16</sup> COM(2025) 47 final - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0047>

## Digital Networks Act (DNA) (Q4 2025)

The Digital Networks Act,<sup>17</sup> which was mentioned among the potential upcoming policy actions already by the White Paper ‘How to master Europe's digital infrastructure needs?’<sup>18</sup>. The Communication ‘Commission work programme 2025’ states that ‘the Digital Networks Act will create opportunities for cross-border network operation and service provision, enhance industry competitiveness and improve spectrum coordination’, aiming to respond to the need for a reliable, ‘high-capacity digital infrastructure’.<sup>19</sup>

## European Business Wallet (Q4 2025)

The European Business Wallet,<sup>20</sup> planned for Q4 2025, aims to ‘simplify business-to-business and business-to-government exchanges for businesses’, according to the Commission work programme 2025. On top of streamlining secure data exchange, the work programme also foresees increased business opportunities for trust service providers stemming from the European Business Wallet. The policy initiative will enrich the European Digital Identity Framework established by Regulation (EU) 2024/1183,<sup>21</sup> and complements and updates the provisions of Regulation (EU) No 910/2014.<sup>22</sup>

### 2.3.2 Upcoming initiatives meant to shape technology

Figure 4 provides a visual overview of the connections between the Technology Roadmap [2] domains and the Research and Innovation Projects under the EUCloudEdgeIoT umbrella. This mapping offers a high-level, bird’s-eye view of the resources being allocated to each topic, and links policy priorities with the ongoing work and research activities contributing to them. For EU policymakers, this dynamic and real-time-updated view can serve as a valuable tool for analysing the topics currently being addressed and for shaping future policies aimed at reinforcing specific areas. This analysis is closely tied to the activities carried out in Work Package 2 (WP2) and will be further detailed and discussed in Deliverable D2.3.

<sup>17</sup> [https://www.europarl.europa.eu/legislative-train/theme-a-new-plan-for-europe-s-sustainable-prosperity-and-competitiveness/file-digital-networks-act-\(dna\)](https://www.europarl.europa.eu/legislative-train/theme-a-new-plan-for-europe-s-sustainable-prosperity-and-competitiveness/file-digital-networks-act-(dna))

<sup>18</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024DC0081>

<sup>19</sup> COM(2025) 45 final - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0045>

<sup>20</sup> <https://www.europarl.europa.eu/legislative-train/theme-a-new-plan-for-europe-s-sustainable-prosperity-and-competitiveness/file-european-business-wallet>

<sup>21</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1183>

<sup>22</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910>



Figure 4. R&D initiatives mapped to the NexusForum.EU R&D roadmap topics

### 2.3.3 Simplification and Implementation

In recent years, the European Commission has introduced several key regulations, including the Data Governance Act,<sup>23</sup> the Data Act,<sup>24</sup> the Cyber Resilience Act,<sup>25</sup> and the Artificial Intelligence Act.<sup>26</sup> However, Europe has faced criticism for having an excessive regulatory framework, which can hinder the competitiveness of companies by delaying their market access compared to regions with more relaxed regulations.

To address this challenge, the Commission has shifted its focus towards bolstering Europe's competitiveness. This involves a radical simplification of the regulatory burden for individuals, businesses, and administrations across the EU. The aim is to create a more streamlined and efficient regulatory environment that supports economic growth and innovation, aligning with the Commission's broader strategy to enhance competitiveness and foster a more integrated Single Market.

The new approach has 4 main guiding blocks, as outlined in the 2025 Communication on implementation and simplification:<sup>27</sup>

<sup>23</sup> (EU) 2022/868 - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0868>

<sup>24</sup> (EU) 2023/2854 - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R2854>

<sup>25</sup> (EU) 2024/2847 - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02024R2847-20241120>

<sup>26</sup> (EU) 2024/1689 - <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

<sup>27</sup> COM/2025/47 final - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0047>

## Ensuring EU policies deliver results

- 1 Preparation and Support for Implementation: The Commission prepares implementation strategies and provides tools like explanatory templates and transposition roadmaps to help Member States anticipate and manage challenges in implementing EU directives.
- 2 Collaboration and Capacity Building: The Commission fosters partnerships between national authorities through expert groups and supports Member States in enhancing their administrative capacity, digital tools, and data through instruments like the Technical Support Instrument.
- 3 Enforcement and Dialogue: Regular implementation dialogues are held to identify implementation issues and opportunities for simplification. If necessary, the Commission takes enforcement action against non-compliant Member States, including referrals to the Court with potential financial sanctions.

## Making Europe simpler and faster

- 1 Competitiveness and Simplification Goals: The European Commission aims to enhance competitiveness by simplifying regulations while maintaining high standards. This involves a 25% reduction in reporting burdens across all administrative costs and a 35% reduction for SMEs, translating to a EUR 37.5 billion cut in recurring administrative costs by the end of the mandate.
- 2 Simplification Tools and Actions: The Commission will utilize tools like omnibus packages to streamline legislation interactions, stress-testing to identify simplification opportunities, and evaluations of laws and policy areas to inform future simplification efforts.
- 3 Engagement and Reality Checks: Reality checks will be conducted to engage with SMEs and small mid-caps, understanding practical challenges and the impact of EU laws on their operations. This feedback will inform simplification measures and future legislative proposal

## Improving how we make new rules

1. Simplified and Effective Legislation: New legislation must be clear, straightforward, and easy to implement, with enforcement and implementation issues addressed from the proposal stage through the legislative process.
2. Impact Assessments and SME Considerations: Systematic SME and competitiveness checks ensure potential impacts on EU companies are identified, with mitigating measures prepared. For delegated and implementing acts, impact assessments or cost analyses are conducted when significant impacts are expected.
3. Reducing Burdens and Streamlining Processes: The Commission applies digital-first principles to reduce reporting burdens and compliance costs. By Q2 2025, it will propose a simple methodology for assessing the impacts of significant legislative amendments without delaying the process.

## Partnership and co-ownership

1. Collaborative Approach: Achieving simplification and implementation goals requires strong commitment from all EU institutions and stakeholders, including the European Parliament, Council, and national, regional, and local authorities. The Commission will work closely with these entities to ensure effective collaboration.

2. Regular Reporting and Accountability: The Commission will maintain transparency and accountability through regular progress reports. Each Commissioner will submit an annual report on implementation and enforcement to the relevant Parliament Committee and Council formation, highlighting progress and areas for improvement.
3. Renewed Interinstitutional Cooperation: The Commission plans to renew the Interinstitutional Agreement on Better Lawmaking to clarify how best to achieve simplification and implementation goals. This will enhance cooperation with the Parliament and Council, ensuring a unified approach to simplifying EU law.

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

#### 3.1 NexusForum.EU approach for increasing awareness on Cognitive Computing Continuum policy initiatives

As part of the NexusForum.EU project's broader mission to shape and inform the evolving policy environment for the Cognitive Computing Continuum (CCC), a comprehensive strategy has been developed to increase awareness of, and meaningful participation in, policy initiatives—particularly those led by the European Commission. The strategy builds on two interlinked approaches: enhancing engagement in formal public consultations and facilitating participatory, co-creative activities that contribute to policy development in a more proactive and inclusive manner.

The approach is built around three core concepts, each with a distinct role and level of stakeholder involvement: **public consultations**, **participatory actions**, and **co-creation and collaborative engagement activities**.

**Public consultations** are formal processes initiated by the European Commission and other EU institutions to collect structured feedback on legislative proposals or strategic initiatives. These consultations are typically open to all, accessible through a dedicated EU platform, and follow a clearly defined format. While crucial for policy legitimacy and transparency, they often require familiarity with legislative language and policy procedures, which can pose a barrier to less experienced stakeholders.

To bridge this gap, NexusForum.EU has introduced **participatory actions**, which are broader engagement measures aimed at increasing understanding, accessibility, and involvement in policy discussions. These actions are designed to raise awareness, build stakeholder capacity, and create a more inclusive entry point for participation. They include outreach campaigns, introductory webinars, simplified policy explainers, and stakeholder mapping exercises. The goal is to equip a diverse set of actors—particularly those unfamiliar with EU policymaking—with the tools and knowledge needed to take part in public consultations or broader policy engagement efforts.

Building on this foundation, **co-creation and collaborative engagement activities** represent a deeper level of stakeholder involvement. These activities are designed not just to inform or consult stakeholders but to actively involve them in shaping policy content. Through interactive methods such as workshops, expert roundtables, collaborative drafting sessions, and policy debates, stakeholders contribute ideas, provide technical expertise, and co-develop policy recommendations. Co-creation differs from participatory actions in that it requires stakeholders to engage more intensively and contribute directly to the formulation of positions, briefs, and strategic documents. These activities also feed directly into the work of NexusForum.EU's Task T3.4, which is responsible for transforming stakeholder input into concrete policy outputs.

To facilitate all three types of engagement, NexusForum.EU has established a central digital infrastructure. The **NexusForum.EU website** serves as the entry point, offering clear explanations about public consultations, their significance, and their connection to topics within the Cognitive Computing Continuum. This includes providing context for policy areas such as AI governance, data sharing, edge computing, and digital sovereignty. Visitors are



encouraged to join the **Whaller platform**, the project's main engagement hub, where they can access detailed resources, discuss current consultations, and participate in interactive policy co-creation processes.

Whaller provides continuously updated information on open consultations, targeted feedback forms, and opportunities for collaboration. It also features a newsfeed mechanism to alert stakeholders to new developments, upcoming deadlines, and emerging EU policy topics relevant to the cloud-edge-IoT continuum. This infrastructure ensures that stakeholders stay informed and are supported throughout their engagement journey.

A strong emphasis is placed on supporting organisations that have never participated in public consultations before. Through tailored guidance, practical resources, and one-on-one outreach, the project aims to demystify the policy process and lower the barriers to entry. Dedicated segments of NexusForum.EU Working Group webinars are also used to build skills in reading consultation texts, formulating effective feedback, and navigating submission portals.

Resources mobilised to implement this strategy include a combination of human, technical, and financial assets. The team comprises moderators, outreach coordinators, policy analysts, and digital support staff. Funding is allocated for digital infrastructure, event delivery, stakeholder communication, and co-creation facilitation. Platforms such as Whaller and communication tools like email newsletters and surveys are employed to keep the stakeholder ecosystem engaged and connected.

To monitor success, NexusForum.EU tracks participation through defined KPIs, including the number of stakeholders engaged, the diversity of participants (with a target of at least ten first-time contributors), and feedback collected from follow-up surveys. These metrics inform adjustments and refinements to the strategy, ensuring that engagement remains responsive and effective.

Therefore, the NexusForum.EU engagement model distinguishes clearly between formal public consultations, broad-based participatory actions, and intensive co-creation processes. Each plays a critical role in empowering stakeholders to engage with policymaking around the Cognitive Computing Continuum. By supporting inclusive awareness-building and deeper policy co-creation, NexusForum.EU ensures that a wide spectrum of perspectives—across sectors, disciplines, and geographies—are meaningfully represented in shaping Europe's digital future.

In alignment with the NexusForum.EU objective to foster policy participation in shaping the Cognitive Computing Continuum, a structured monitoring of relevant EU-level public consultations has been implemented. The consultations tracked below reflect ongoing and forthcoming policy initiatives with direct relevance to the cloud-edge-IoT ecosystem, digital sovereignty, AI, data spaces, and cybersecurity.

## 3.2 Identified public open consultations

NexusForum.EU has identified 14 consultations relevant to the project's scope and encouraged the community to participate. These consultations are categorised into three groups: active, closed, and upcoming.

Table 2. Policy related open consultations

#	Related Policy/legislation	Link	Status	Consultation deadline	Date published
1	'GreenData4All' initiative	<a href="#">Link</a>	Active	30.04.2025	12.02.2025
2	Directive 2014/23/EU on the award of concession contracts; Directive 2014/24/EU on public procurement; Directive 2014/25/EU on procurement by entities operating in the water, energy, transport and postal services sectors.	<a href="#">Link</a>	Closed	07.03.2025	05.02.2025
3	Preparatory work for the next MFF on competitiveness (from 2027)	<a href="#">Link</a>	Active	06.05.2025	19.02.2025
4	Interoperability regulatory sandboxes, introduced by the Interoperable Europe Act (Regulation (EU) 2024/903)	<a href="#">Link</a>	Closed	15.03.2025	26.02.2025
5	A European Strategy for AI in science – paving the way for a European AI research council	<a href="#">Link</a>	Upcoming		TBA (Q3 2025)
6	European Data Union Strategy	<a href="#">Link</a>	Upcoming		TBA (Q1 2025)
7	The EU Cybersecurity Act	<a href="#">Link</a>	Upcoming		TBA (Q1 2025)
8	European strategy on research and technology infrastructures	<a href="#">Link</a>	Upcoming		TBA (Q3 2025)
9	International Digital Strategy	<a href="#">Link</a>	Upcoming		TBA (Q2 2025)
10	European Innovation Act	<a href="#">Link</a>	Upcoming		TBA (Q1 2026)
11	European Research Area Act	<a href="#">Link</a>	Upcoming		TBA (Q3 2026)
12	Apply AI Strategy	<a href="#">Link</a>	Active	04.06.2025	09.04.2025
13	Cloud and AI Development Act	<a href="#">Link</a>	Active	04.06.2025	09.04.2025
14	EU cybersecurity certification – amendment to the scheme on common criteria	<a href="#">Link</a>	Upcoming		

NexusForum.EU partners have promoted these opportunities via Whaller and the project's newsfeed mechanism, supported by simplified summaries and working group discussions. Targeted stakeholder engagement has been initiated to encourage meaningful input from underrepresented sectors.



👉 This is your chance to have a say in the interoperability regulatory sandboxes, introduced by the Interoperable Europe Act!

The public consultation is open until the 13th of March 2025 <sup>10h</sup> 17



Figure 5. Whaller publication of one online consultation

These consultations are being tracked as part of NexusForum.EU's effort to support increased participation in digital policy development. Relevant materials—such as explainers, timelines, and discussion threads—are continuously updated and shared via the NexusForum.EU website and Whaller platform.

To assess the level of engagement and actual participation of the NexusForum.EU Community in the identified public consultations, a dedicated survey will be developed and disseminated via the project's communication channels, including Whaller and the project newsletter. The survey will aim to capture whether stakeholders have submitted feedback, the nature of their contributions, perceived barriers to participation, and interest in future policy engagement.

## 4 EU Open Source, Standardisation, and Skills Development initiatives

Open Source plays a pivotal role in reinforcing the European Union's digital sovereignty by empowering the continent to build, control, and innovate upon its own digital infrastructure. As the EU strives to establish a secure, resilient, and competitive digital ecosystem, the adoption and development of open-source technologies across the European cloud computing continuum—spanning edge, fog, and cloud layers—has emerged as a strategic enabler. This section explores how Open Source supports the EU's path toward digital autonomy, with a focus on its role in the agricultural sector, as a follow-up and complement to the earlier case study on the automotive industry presented in D3.1 [1]. It also addresses the significance of standardisation in ensuring interoperability and trust in open source solutions, and highlights the importance of skills development through initiatives such as the EU Open Source Academy. Together, these elements form a robust foundation for advancing the EU's digital autonomy and ensuring long-term technological leadership.

### 4.1 Case Study: Open Source in Agriculture

#### Introduction – the role of OSS in enabling a sovereign agriculture sector in Europe

In February 2025, the European Commission published its *Vision for Agriculture and Food*, a strategic roadmap to ensure that Europe's agri-food systems are competitive, resilient, and future-oriented. The document places strong emphasis on the digital transformation of agriculture as a lever for achieving sustainability, food security, and innovation, particularly against the backdrop of growing geopolitical uncertainty. In this context, Open Source software (OSS) can play a role in accelerating digital uptake, enabling transparency, adaptability, and cost-efficiency – elements that are vital to building a resilient European food system.

Despite the growing recognition of OSS as a driver of innovation and collaboration, its uptake in agriculture remains more limited than in sectors like automotive.<sup>28</sup> Agriculture's highly fragmented landscape – composed of smallholder farmers, cooperatives, agribusinesses, and technology providers – presents a challenge to cohesive digital innovation. Nevertheless, aligning OSS with Europe's sustainability, data, and digitalisation strategies presents a significant opportunity to support fair, resilient, and competitive farming systems.

Recent EU initiatives such as the *Farm to Fork Strategy*, the *European Data Strategy*, and the post-2022 *Common Agricultural Policy* have underlined the importance of digital and data-driven solutions. Open source contributes to these goals by reducing barriers related to affordability, interoperability, and vendor lock-in – especially in rural and resource-constrained areas where digital access is uneven.

#### Background

Europe's agricultural sector employs 20 million people and provides food to over 500 million consumers<sup>29</sup>. The sector is under pressure to boost efficiency and sustainability, but its transformation is hindered by increasing technological lock-in. Farmers and their data are

<sup>28</sup> <https://newsroom.eclipse.org/news/announcements/vision-paper-open-source-software-automotive-industry>

<sup>29</sup> <https://op.europa.eu/publication-detail/-/publication/f08f5f20-ef62-11e6-8a35-01aa75ed71a1>

often tied to proprietary systems dominated by large agribusinesses and tech giants, who typically show little interest in interoperability.<sup>30</sup> This lock-in extends down the supply chain to buyers and retailers, reinforcing dependence on incumbent platforms.

Smallholder farmers, who make up the majority of European producers, face particular challenges. Limited financial resources, low digital literacy, and a strong cultural attachment to traditional practices hinder their ability to adopt new technologies. As one interviewee noted, "There is no money in agri[culture]... the big players who have the margins are happy to buy from big suppliers."

Public research funding and subsidies have proven to be key enablers for OSS in agriculture, often including open-source dissemination requirements. However, many projects struggle with sustainability after initial funding ends, leaving valuable tools undermaintained or abandoned. Nonetheless, a growing number of initiatives, both in OSS and OSH<sup>31</sup>, address key use cases such as Automation and Robotics, Farm Management Systems, and Remote Sensing and Imagery<sup>32</sup>.

### Barriers and Enablers to OSS Adoption

Key barriers to OSS adoption in agriculture include:

- **Affordability and skills gaps:** Many farmers, especially on small and mid-sized farms, lack both the resources and digital literacy to adopt new technologies.
- **Connectivity constraints:** Rural areas often lack reliable internet, limiting the usefulness of cloud-based systems and increasing interest in edge or hybrid models.
- **Trust and control:** Proprietary "black-box" systems create mistrust and raise concerns about data ownership and transparency.
- **Fragmentation in standards and governance:** The absence of common standards for data interoperability impedes long-term collaboration and reuse.

OSS-based digital applications, especially when co-developed with end users and backed by strong policy frameworks, offer a pathway to overcome these challenges.

### Key stakeholders and initiatives:

- **AgStack<sup>33</sup>** – Focused on facilitating OSS development improving global efficiency of the agriculture sector. Positioned under the broader umbrella of the Linux Foundation signal. Members, however, mainly include Software technology companies, associations and research actors, less the more established incumbents in the space. Current focus is reportedly on how commodities can be tracked and traced through supply chains, proving point of origin to, e.g., limit deforestation, and promote sustainable farming.

<sup>30</sup> <https://doi.org/10.1177/20539517241306365>

<sup>31</sup> <https://horizon-openagri.eu/open-source-catalogue/>

<sup>32</sup> <https://github.com/brycejohnston/awesome-agriculture>

<sup>33</sup> <https://agstack.org/>

- **OpenAgri<sup>34</sup>** – An EU-funded project focused on developing and providing open-source agricultural digital solutions (ADSs) to empower farmers, especially in remote areas with limited connectivity. By fostering collaboration among farmers, technology developers, and other stakeholders, OpenAgri aims to create sustainable and practical tools tailored to real-world agricultural challenges. They have a close collaboration with the AgStack foundation, looking to establish their projects<sup>35</sup> in the foundation to increase sustainability.
- **QuantiFarm<sup>36</sup>** – An EU funded project focused on assessing the impact of digital agricultural technologies (DATS) on sustainability in farming practices. It aims to understand how these technologies are adopted and integrated on farms, considering both quantitative and qualitative aspects. Tools and platforms developed for the purpose are generally available as OSS<sup>37</sup>.
- **Farmtopia<sup>38</sup>** – An EU funded project aimed at democratizing digital farming by making Agricultural Digital Solutions (ADSs) accessible and affordable for small-scale farmers. The project focuses on co-creating, deploying, and piloting innovative ADSs through 18 Sustainable Innovation Pilots (SIPs), aiming to enhance economic and environmental outcomes in agriculture. Farmtopia also works on reducing costs by developing reusable OSS modules and scalable infrastructure, ensuring that digital farming solutions effectively address the needs of small farms<sup>39</sup>.

#### Examples of ongoing Open Source projects:

- **FarmOS<sup>40</sup>** - a web-based application for farm management, planning, and record keeping. It is developed by a community of farmers, developers, researchers, and organizations with the aim of providing a standard platform for agricultural data collection and management. The farmOS server is built on top of Drupal, which makes it modular, extensible, and secure. The farmOS Field Kit app provides offline data entry.
- **FarmBot<sup>41</sup>** - an OSS and OSH project that automates small-scale farming using a Cartesian coordinate robot to plant, water, and monitor crops. It is controlled through a web-based interface, allowing users to manage their gardens efficiently. Arduino plays a crucial role in FarmBot by providing the hardware and software framework for controlling the robot. Arduino micro-controllers are used to interface with various sensors and actuators, enabling precise control over farming tasks. This integration

---

<sup>34</sup> <https://horizon-openagri.eu/>

<sup>35</sup> <https://horizon-openagri.eu/os-solutions/>

<sup>36</sup> <https://quantifarm.eu/about/>

<sup>37</sup> <https://gitlab.com/QuantiFarm>

<sup>38</sup> <https://farmtopia.eu/>

<sup>39</sup> <https://gitlab.com/Farmtopia>

<sup>40</sup> <https://farmos.org/>

<sup>41</sup> <https://docs.farm.bot/>

allows FarmBot to perform automated actions based on real-time data, such as soil moisture levels and weather conditions

### Enhancing Supply Chain Transparency Through Open Source Digital Traceability

Traceability is becoming a cornerstone of sustainability and regulatory compliance in the agri-food sector. This is particularly true following the adoption of the EU Deforestation Regulation (EUDR), which requires operators placing certain commodities (such as soy, palm oil, beef, and coffee) on the EU market to prove that these are not linked to deforestation or forest degradation.<sup>42</sup> The EUDR marks a significant regulatory shift, compelling agri-food stakeholders to collect, manage, and validate geospatial and supply chain data to comply with the due diligence obligations.

Open source digital tools and platforms offer promising solutions to meet these challenges. Systems like INATrace provide low-cost, modular infrastructure that can be adapted to a variety of local contexts and integrated across stakeholders. These tools can increase transparency, lower barriers for adoption among smallholder producers, and improve interoperability through shared standards. Crucially, they can support the kind of decentralized data management needed for cross-border compliance with the EUDR, without locking stakeholders into proprietary ecosystems.

The regulation also incentivises improvements in data collection and sharing practices at the farm and cooperative level, where many producers still lack digital infrastructure. Open source traceability platforms – supported by collaborative development models – can facilitate capacity-building and strengthen the position of producers in the value chain. They also make it easier for downstream actors, including buyers and regulators, to verify claims about the origin and sustainability of agricultural goods.

Ultimately, the intersection of EUDR compliance and Open Source digital infrastructure is not just a technical question, but also a matter of digital sovereignty, equity, and resilience in global supply chains. Global initiatives like the Digital Integration of Agricultural Supply Chain Alliance (DIASCA) are working towards advancing Digital Public Infrastructure (DPI) for sustainable agricultural supply chains. In response to the fragmentation and lack of interoperability among digital tools, the alliance aims to build a more cohesive, accessible, and efficient ecosystem – based on open standards, clear enabling frameworks, shared governance models, and open-source system architecture.

## 4.2 Empowering Digital Sovereignty: The Role of a Skilled Open Source Workforce and the EU Open Source Academy

A skilled workforce in Open Source is essential to achieving European digital sovereignty, as it empowers the EU to develop, maintain, and adapt its own digital infrastructure without reliance on proprietary systems or external vendors. By fostering expertise in open-source technologies, Europe can ensure transparency, security, and long-term control over critical digital systems, especially in strategic sectors such as cloud computing, artificial intelligence, and the Internet of Things.

The EU Open Source Academy ([www.europeanopensource.academy/](https://www.europeanopensource.academy/)) is an initiative promoted by the EC which runs in parallel to NexusForum.EU, that plays a vital role in this

<sup>42</sup> <https://www.sustainable-supply-chains.org/topics/digitalisation-traceability/>



context contributing significantly to the development of a skilled and self-reliant digital workforce, supporting the EU's broader goals of digital autonomy and technological leadership.

Inspired by the world's leading academies of science, the EU Open Source Academy is envisioned as a lighthouse for Open Source in Europe, serving as a strategic and influential institution that promotes the value, innovation, and sustainability of Open Source technologies across the continent. The Academy is designed to be a central hub for knowledge, **advocacy**, and recognition, bringing together developers, businesses, policymakers, and academic institutions to strengthen Europe's digital sovereignty and technological independence.

At its core, the EU OS Academy is committed to raising awareness of the strategic and economic importance of Open Source in shaping Europe's digital future. It aims to educate and inform European business leaders and policymakers about the critical role of Open Source in modern digital infrastructure, from cloud computing and artificial intelligence to public services and industrial innovation. By doing so, the Academy supports the EU's broader objectives of technological self-reliance, competitiveness, and resilience in an increasingly interconnected and digital world.

A key initiative of the Academy is the annual European Open Source Awards, which celebrate and recognize excellence in the Open Source field. These awards honor individuals, organizations, and projects that have made significant contributions to the European Open Source ecosystem—whether through code development, innovative business models, or policy advocacy. The Awards also serve as a platform for community engagement, bringing together Open Source stakeholders to collaborate, share best practices, and advocate for the interests of the Open Source community.

### 4.3 Standards

As of May 2025, the European Union's Cyber Resilience Act (CRA) is progressing through its implementation phase, with a focus on developing harmonized cybersecurity standards for products with digital elements. The CRA, which entered into force in December 2024, mandates that manufacturers ensure cybersecurity throughout the lifecycle of their products, with full obligations applying from December 2027.

The Open Source community is actively involved in shaping these standards. The Open Source Security Foundation (OpenSSF), in collaboration with the Linux Foundation Europe, has launched initiatives to assist Open Source projects in aligning with CRA requirements. This includes the release of the Open Source Project Security Baseline, a framework outlining best practices for Open Source software security, and educational resources such as the free course "Understanding the EU Cyber Resilience Act (CRA)" to raise awareness and preparedness among developers.

Additionally, the Eclipse Foundation has established the Open Regulatory Compliance Working Group to facilitate the development of common specifications for secure software development based on Open Source best practices. These collaborative efforts aim to ensure that Open Source software can meet the CRA's cybersecurity requirements, thereby maintaining its integral role in the digital ecosystem.



## 5 Suggestion of new policy initiatives and decisions: Analysing the factors

### 5.1 Co-creating the SWOT Analysis

During this phase of the project, we conducted an in-depth analysis of the six key factors previously identified as crucial for shaping EU technological sovereignty and the convergence of Edge, Cloud, and IoT technologies.

This analysis was achieved through a SWOT framework examining Strengths, Weaknesses, Opportunities, and Threats of the EU in each of the identified factors that are critical for the EU digital sovereignty and the deployment of Edge, Cloud, and IoT technologies. These factors, which are further described in Deliverable D3.1, are:

- **F1:** Technology, innovation and research capabilities
- **F2:** Framework conditions (policies, strategies, plans, regulations, etc.)
- **F3:** Enabling conditions (Open Source, open standards, skills and ethics)
- **F4:** Infrastructures and connectivity (including space infrastructure and data)
- **F5:** Collaboration & engagement between initiatives at EU and international level
- **F6:** Industry participation

This approach enables us to build on existing strengths, capitalize on opportunities, and at the same time, address weaknesses and mitigate potential threats.

#### 5.1.1 Analytical Approach and Implementation Process

The approach adopted is dynamic and iterative, centered on stakeholder engagement and expert consultation. It combines insights derived from the project tasks with contributions from industry representatives, researchers, and policymakers.

The SWOT analysis done is based on both secondary sources and primary data, gathered through:

- Desk research, which included key reports such as:
  - “The Future of European Competitiveness” report released by Mario Draghi in September 2024 and
  - “Much More Than a Market: Speed, Security, Solidarity” by Enrico Letta, presented to the European Council on 18 April 2024.
- Primary sources, including the conclusions of the workshop we held during the NexusForum.EU2024 Summit (19-20 September 2024, Brussels), which laid the groundwork for the six online thematic working sessions held, one for each key factor.

Each factor has been analyzed in 6 separate working sessions held between January and March 2025, involving partners responsible for the most relevant project tasks, fostering co-creation and ensuring that the SWOT analysis reflected both technical knowledge and strategic insights.

#### 5.1.2 SWOT Dimensions

Table 3. SWOT Analysis dimensions

<b>1 Strengths</b> (internal perspective)	<b>2 Weaknesses</b> (internal perspective)
<b>3 Opportunities</b> (external perspective)	<b>4 Threats</b> (external perspective)

This work took place between months 9 and 18 of the project. Since it has been conducted in parallel with ongoing activities, some tasks, such as those related to international collaborations with South Korea, Canada, and New Zealand, are not yet fully developed and are therefore only partially reflected in the analysis. However, collaboration with Japan has progressed significantly and is included more extensively in the SWOT analysis.

Although it is too early to draw final conclusions from the SWOT, some preliminary findings and key insights have emerged from the SWOT and have been validated in collaboration with the project partners.

### 5.1.3 Results of swot analysis

## F1: TECHNOLOGY, INNOVATION AND RESEARCH CAPABILITIES



Figure 6. SWOT analysis for F1-Technology, innovation and research capabilities

## F2: FRAMEWORK CONDITIONS (policies, strategies, plans and regulations)

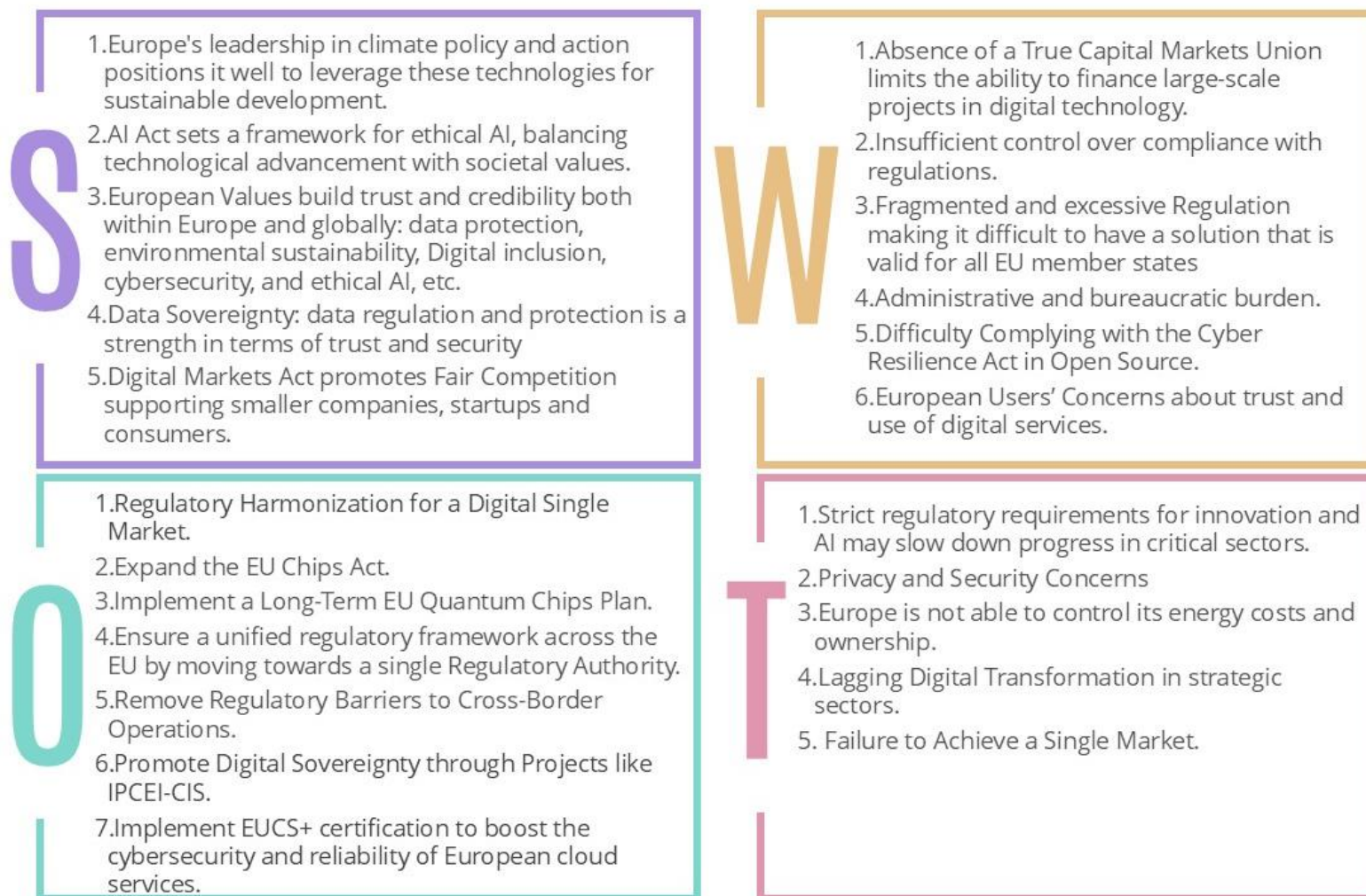


Figure 7. SWOT analysis for F2 Framework conditions (policies, strategies, plans, regulations, etc.)-



### F3: ENABLING CONDITIONS (open source & standards, skills, ethics)

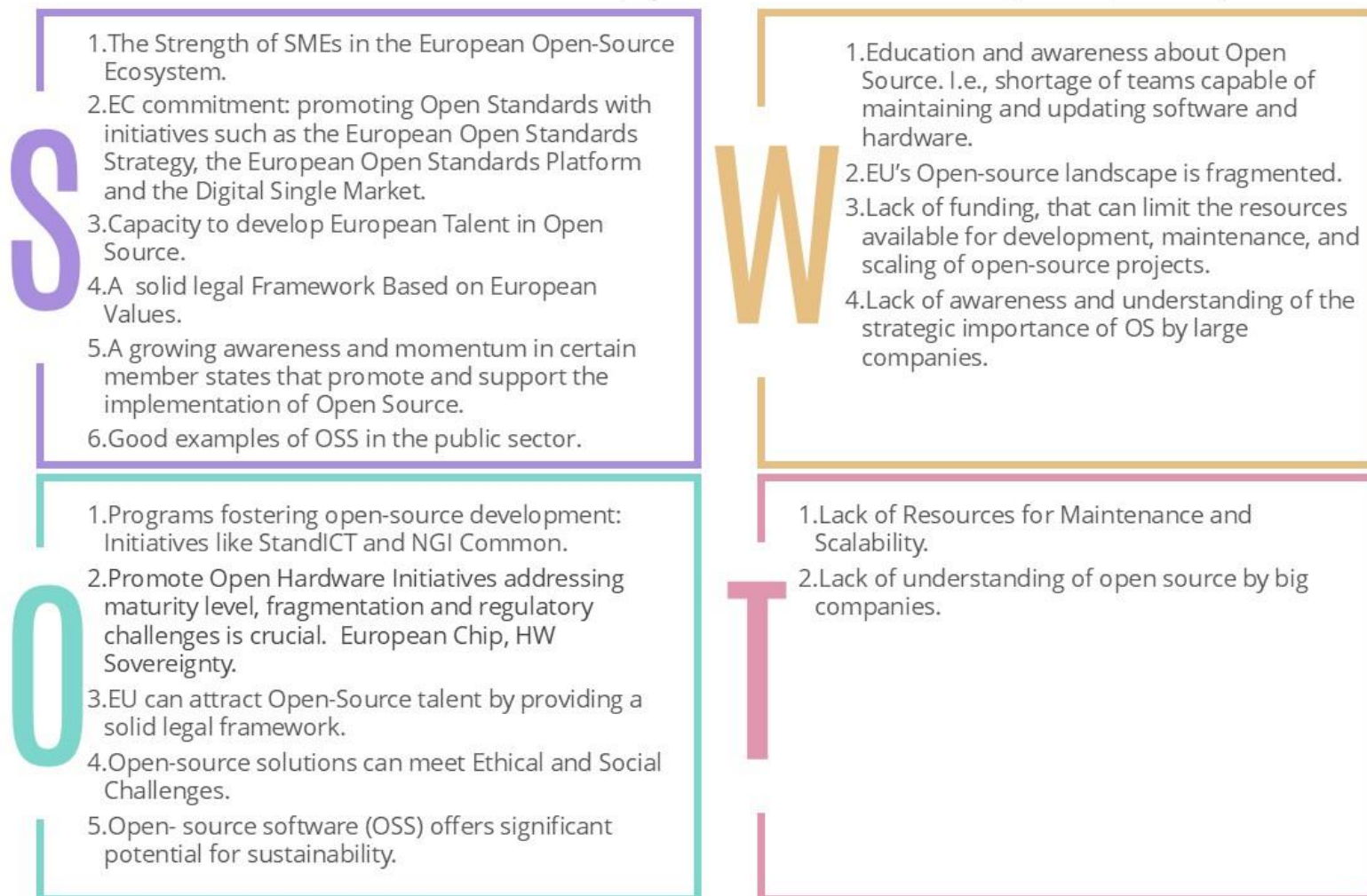


Figure 8. SWOT analysis for F3 Enabling conditions (Open Source, open standards, skills and ethics)-

## F4: INFRASTRUCTURES & CONNECTIVITY

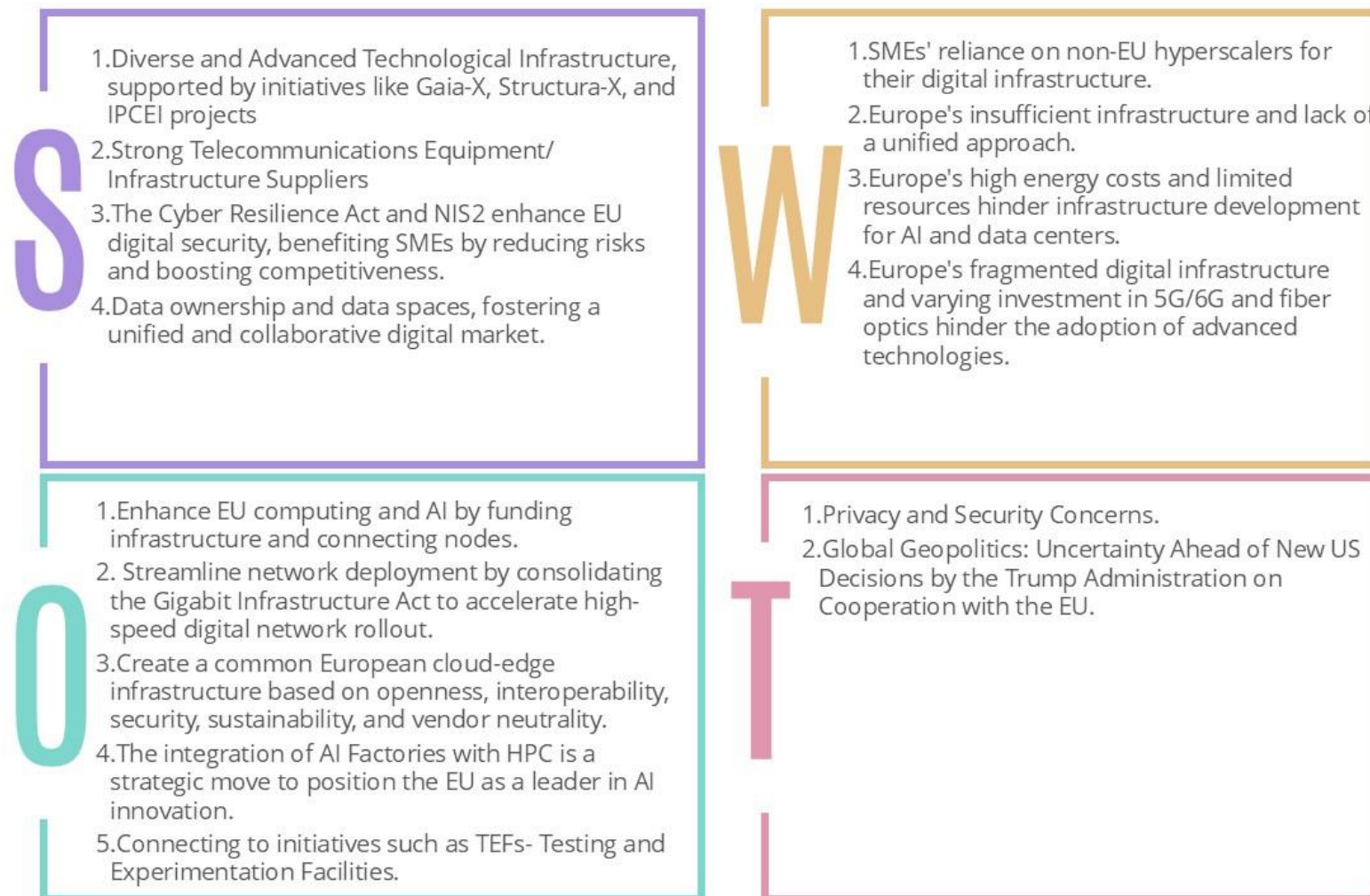


Figure 9. SWOT analysis for F4 Infrastructures and connectivity (including space infrastructure and data)-



## F5: COLLABORATION & ENGAGEMENT

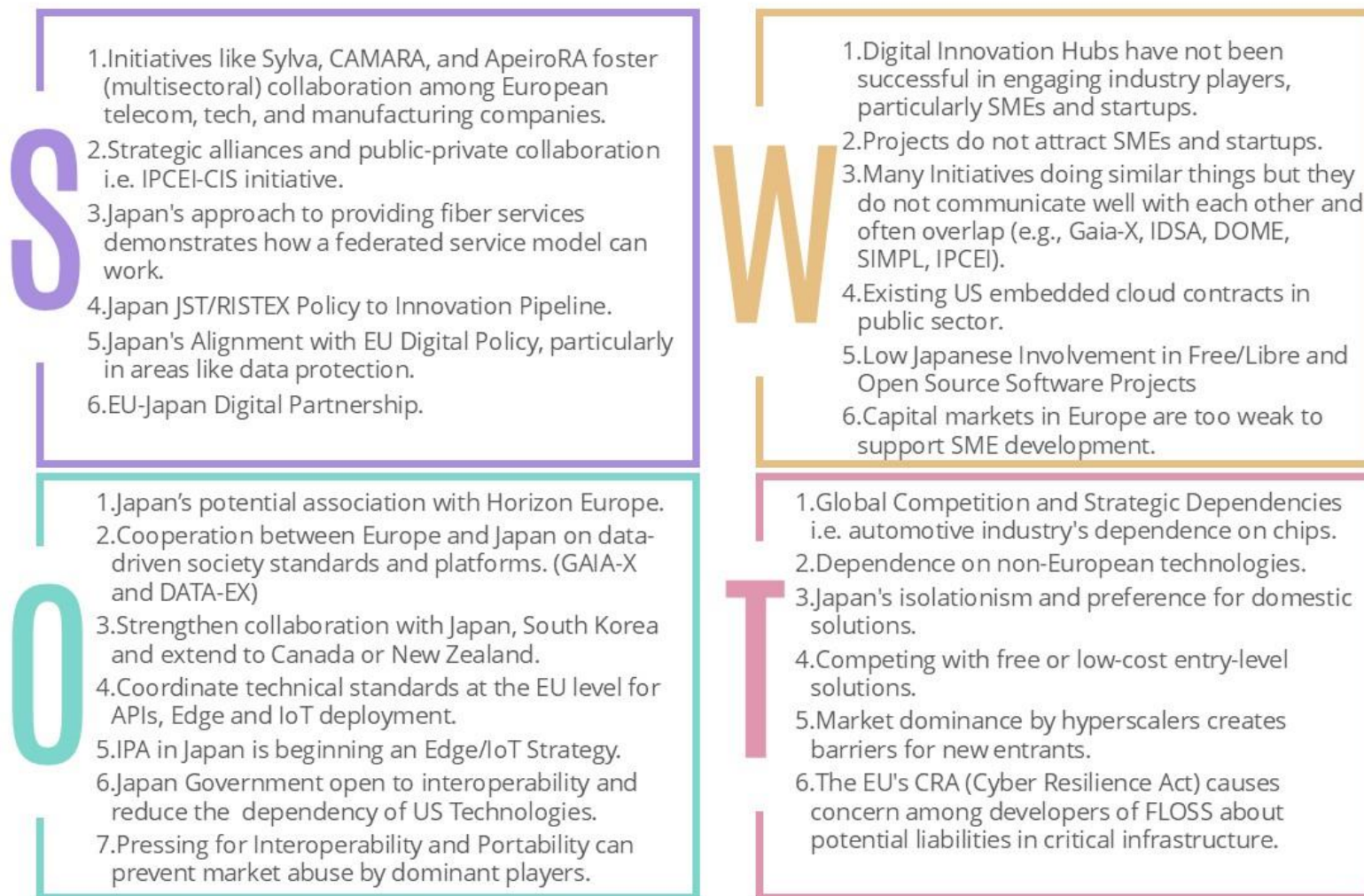


Figure 10. SWOT analysis for F5 Collaboration & engagement between initiatives at EU and international level

## F6: INDUSTRY

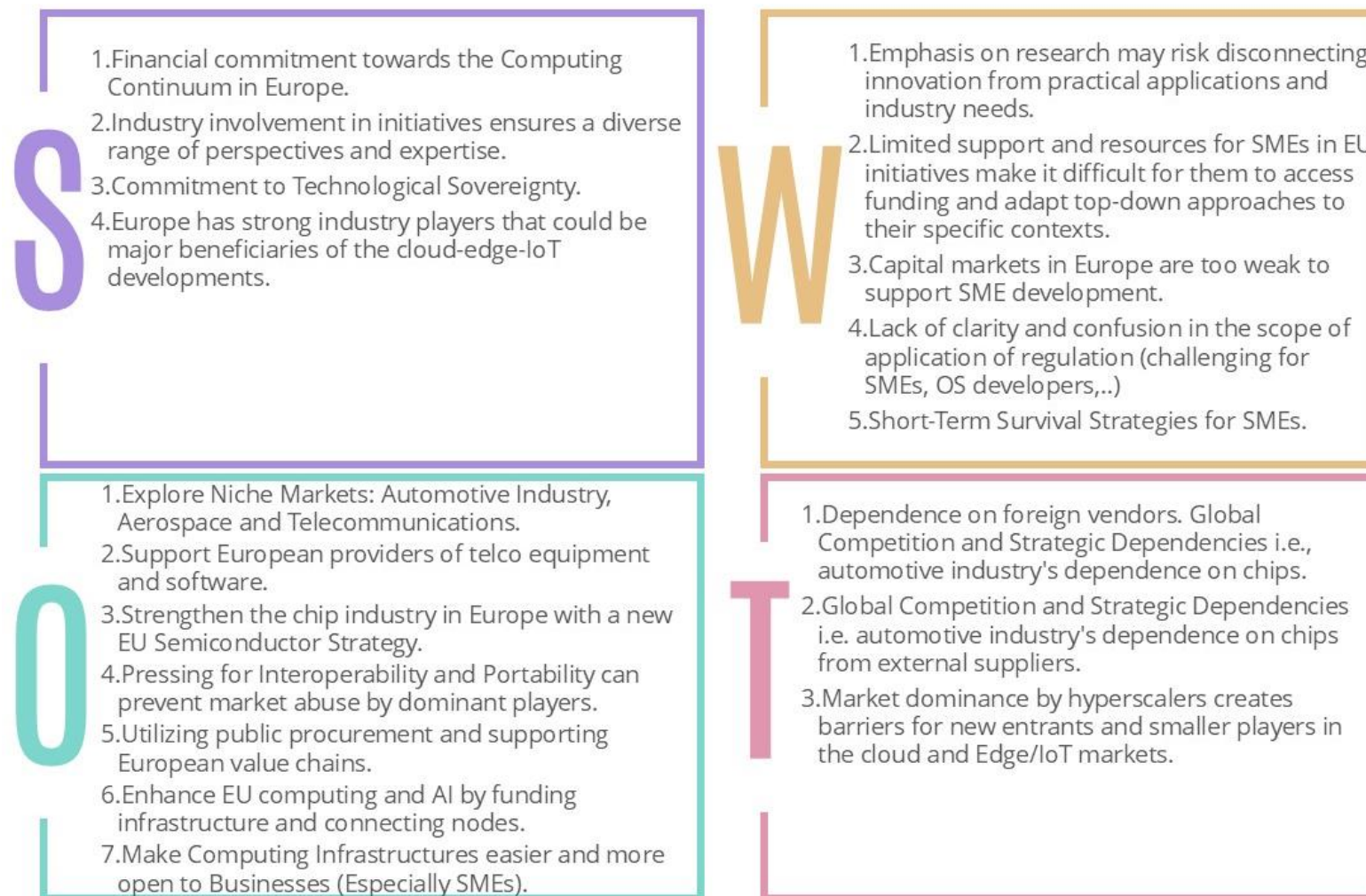


Figure 11. SWOT analysis for F6 Industry participation

### 5.1.3.1 Main Findings

Based on the interviews conducted with partners and the SWOT analyses performed, we can **highlight the following key areas**, among others, where the EU computing continuum should focus and advance to achieve consolidation and technological sovereignty:

- 1) **The development of a Federated Technologies Ecosystem within the computing continuum, encompassing edge, cloud, and IoT technologies, represents a significant opportunity for Europe to integrate and optimize dispersed resources.** This initiative aims to create a seamless and interconnected environment where data and computational tasks can be efficiently managed across various platforms and devices. By fostering collaboration among diverse stakeholders, Europe can leverage this ecosystem to enhance its digital infrastructure, promote innovation, and maintain competitive advantage in the global market.

A Federated Technologies Ecosystem would have the potential advantages such as: Enhanced Resource Utilization by integrating edge, cloud, and IoT technologies, a federated ecosystem could ensure that computational and data resources are used more efficiently; Increased Collaboration between smaller entities and larger organizations. This is particularly beneficial for startups and SMEs, which can leverage the infrastructure and expertise of larger companies to innovate and scale their solutions; Strengthening Digital Sovereignty by keeping data and technological infrastructure under European control, a federated ecosystem could enhance security and compliance with EU regulations; Scalability and Flexibility: Federated systems are designed to be inherently scalable and flexible. This means they could adapt to changing demands and integrate new technologies; and last, developing a federated ecosystem can enhance the global competitiveness of European technology providers. By fostering innovation and improving resource utilization, European companies can offer more advanced and efficient solutions.

- 2) **The implementation of the European Data Strategy presents a significant opportunity to create a single market for data, ensuring Europe's global competitiveness and data sovereignty.** This strategy aims to facilitate the free flow of data within the EU and across various sectors, benefiting businesses, researchers, and public administrations. By establishing clear and fair rules for data access and reuse, the strategy promotes innovation and growth, positioning Europe as a leader in the global data-driven economy. The creation of Common European Data Spaces is expected to make available for use in the economy and society while keeping the entities that generate the data in control.

One of the key benefits of this strategy is enhanced resource utilization. Additionally, the strategy strengthens digital sovereignty by ensuring that European data and technological infrastructure remain under European control, enhancing security and compliance with EU regulations. This is crucial for protecting sensitive data and maintaining trust among citizens and businesses.

Moreover, the European Data Strategy fosters market competitiveness by making European technology providers more attractive globally. By promoting data-driven innovation and creating a dynamic and secure data economy, European companies can offer advanced and efficient solutions, enhancing their global market position.

- 3) **Establishing a coordinated strategy to support open-source maintenance, scalability, and skills development is crucial for overcoming fragmentation and strengthening the sustainability of the Computing Continuum ecosystem.** This

strategy aims to unify efforts across various stakeholders, including developers, organizations, and educational institutions, to ensure that open-source projects are well-maintained and scalable.

The benefits of such a coordinated strategy are manifold. Firstly, it enhances resource utilization by pooling efforts and knowledge, leading to more efficient and sustainable development practices. This can result in faster innovation cycles and reduced duplication of efforts, ultimately accelerating technological advancements. Secondly, it promotes inclusivity and collaboration, allowing smaller entities and individual contributors to participate alongside larger organizations, thereby democratizing access to technological resources and opportunities. Furthermore, a well-supported open-source ecosystem can improve market competitiveness by fostering a culture of continuous improvement and adaptability, making European technology providers more resilient and innovative in the global market. Overall, this strategy is essential for building a robust and sustainable Computing Continuum ecosystem that can thrive in the face of evolving technological demands.

Overcoming fragmented regulatory frameworks and increasing awareness of the strategic importance of open-source governance, particularly among large companies and public institutions, are key challenges for the EU. Addressing these issues would enable a more coherent and effective approach to open-source in the Computing Continuum.

- 4) **Advancing a unified, open, and secure EU digital infrastructure is essential to supporting the development of AI factories.** Enhanced connectivity and security will provide AI factories with the resources needed to develop cutting-edge AI models and applications. This infrastructure can facilitate among supercomputing centers, universities, SMEs, and industry, advancing AI in sectors like healthcare, manufacturing, climate, finance, and space. Integrating AI Factories with High-Performance Computing (HPC) represents a strategic opportunity to strengthen Europe's AI capabilities and reduce dependence on external technologies. Leveraging HPC resources allows AI Factories to develop and deploy advanced AI models more efficiently, fostering innovation and collaboration across various sectors.

The benefits of this unified digital infrastructure are manifold. Firstly, it has the potential to reduce the time and cost associated with training complex AI models, making AI development more accessible and efficient. Secondly, it will enhance Europe's digital sovereignty by ensuring that AI innovations are developed and maintained within the EU, adhering to European values and regulations. This is crucial for maintaining trust and security in AI applications. Additionally, a unified infrastructure will promote scalability and flexibility, allowing AI factories to adapt to evolving technological demands and integrate new advancements seamlessly. Ultimately, this initiative could strengthen Europe's position in the global AI landscape fostering a competitive and innovative AI ecosystem that can drive economic growth and societal progress.

- 5) **Prioritizing strategic cooperation with like-minded countries such as Japan, South Korea, and Canada is a necessary step to build an open, sovereign, and competitive cloud and edge infrastructure in Europe.** Existing collaborations, such as the EU-Japan Digital Partnership and Japan's alignment with EU digital policies, already demonstrate strong potential for alignment. Moreover, opportunities for technical cooperation on data-driven platforms (e.g., GAIA-X, DATA-EX), interoperability standards, and shared approaches to data protection can reinforce mutual strengths and promote innovation.

By joining forces with trusted international partners, the EU can address current challenges more effectively, including market fragmentation, low SME engagement, and dependency



on non-European technologies. These alliances can offer complementary capabilities and foster dynamic ecosystems that attract startups and scale-ups. In addition, international cooperation aligned with democratic values strengthens the EU's position against dominant non-EU hyperscalers and supports a resilient digital infrastructure built on openness, trust, and shared sovereignty.

- 6) **The implementation of a new EU semiconductor strategy is essential to bridge the gap between Europe's digital ambitions and the industrial realities of the Cognitive Computing Continuum, particularly for SMEs.** The SWOT analysis highlights strong dependencies on non-European technologies, strategic vulnerabilities in global chip supply, and weak capital markets that hinder SME competitiveness. A robust and forward-looking semiconductor strategy would help reduce these risks, improve technological sovereignty, and ensure that European companies, especially SMEs, have access to affordable, secure, and locally produced components.

**Moreover, aligning this strategy with collaborative efforts involving like-minded countries, interoperability initiatives, and EU-wide standardization could amplify its impact across the Cloud, Edge, and IoT spectrum.** It would enable Europe to better coordinate industrial and innovation efforts, stimulate cross-border investment, and create a more resilient and inclusive ecosystem for the next generation of digital technologies. For SMEs in particular, this would mean lower barriers to innovation, greater strategic autonomy, and enhanced participation in shaping Europe's digital future.

- 7) **Simplifying and harmonizing digital regulations across the EU is a key enabler for creating a truly competitive Digital Single Market and unlocking innovation across the Cloud, Edge, and IoT domains.** The SWOT analysis points to excessive regulatory fragmentation, administrative burdens, and lack of harmonization across Member States as major obstacles for companies, particularly SMEs. These issues not only increase compliance costs but also hinder cross-border operations and slow down digital transformation in strategic sectors.

**A unified, streamlined regulatory environment would reduce barriers for market entry, improve legal certainty, and foster trust in digital services.** Opportunities such as expanding and reviewing the EU Chips Act, promoting digital sovereignty, and establishing a unified cybersecurity and regulatory framework can help address these challenges. Moreover, this would reinforce Europe's strengths in ethical AI, data protection, and digital trust, while empowering innovation and growth through fairer, more predictable conditions for all actors in the ecosystem.

#### 5.1.4 Next steps

The main highlights will be discussed and validated through dedicated Working Groups, enabling a more precise and shared understanding of the priority topics that must be addressed to advance Continuum Computing in the EU.

These topics will then be presented at the upcoming NexusForum.EU 2025 Summit, where the intention is to confirm the strategic direction and fine-tune the framing of the topics. While no major shifts are expected, this step will ensure that all relevant perspectives are taken into account and that the outcomes enjoy broad support across the Community.

This phase will be carried out in close coordination with task leaders to ensure consistency with ongoing activities and to effectively integrate the outcomes into the respective Working Groups and Summit deliverables.

Building on this process, the insights gathered will serve as the basis for translating the findings into concrete policy and strategic recommendations. These will aim to foster the convergence of cloud, edge, and IoT computing, while strengthening Europe's digital sovereignty.



## 6 Digital Sovereignty in the international context

As mentioned in the previous sections, the international collaboration is a distinctive characteristic of NexusForum.EU, thanks to the two consortium partners from Japan (Meiji University) and the Republic of Korea (Yonsei University) and the collaboration with other EU initiatives<sup>43</sup>, in particular, the [INPACE project](#).

INPACE is designed around Thematic Working Groups (TWGs) for boosting the collaboration between EU and the Indo-Pacific region, which includes the two NexusForum.EU target countries, Japan and the Republic of Korea. One of this TWG is focusing to the Cloud Computing Continuum with the name Cloud-Edge-IoT and Martel is the partner managing it, while OpenNebula is among the experts group. This allowed a strong collaboration between the two projects and the joint organisation of a flagship event in Tokyo on March 31st 2025, as part of the EU-Japan Digital Week, with the name "Smart Connectivity and Computing Workshop", in which several experts from EU and Japan gather together to discuss key elements of the collaboration between the two regions. One milestone in the event was the feedback on the NexusForum.EU Research and Innovation Roadmap, whose results are available online and highlight a commonalities of interest between EU and Japan on topics like *emerging areas such as edge computing, data spaces and quantum computing and the importance of technological sovereignty, viewing it as a critical factor for both regions' smart connectivity and computing ecosystems*: <https://eucloudedgeiot.eu/the-eu-japan-cognitive-computing-continuum-complementarity-and-challenges-for-the-way-forward/>.

Another milestone in the event was the discussions during the workshop sessions (<https://egcp.enrich-global.eu/communities/inpace/events/smart-connectivity-and-computing-workshop>), which presented the numerous initiatives that are linking EU and Japan and are helping to reinforce each region's digital sovereignty leveraging collaboration and cooperation on strategic topics and initiatives. Key initiatives and collaborations are currently in the fields of Data Spaces, HPC and AI and include:

- The signature of several Memorandum of Understanding (MoU) e.g between the Data Society Alliance (Japan) with European organisations like FIWARE, IDSA, GAIA-X, Manufacturing-X and ongoing project in the Data Spaces field e.g. CIRPASS-2 on Digital Product Passport or Data4Industry-X on Industrial Collaboration.
- The scientific exchange and common architecture in the HAMANI project to boost the research and implementation on HPC infrastructures between EU and Japan
- The development of Trusted Frameworks for data sharing leveraging Data Spaces and Federated AI algorithms to preserve data sovereignty and control by minimising data transfer.

It is important to highlight how most of these initiatives relies on Open Standards and Open Source Software (OSS) as a way to increase Digital Sovereignty and reduce "digital deficit". In a recent report on Japanese strategy for Open Source,<sup>44</sup> the term "digital deficit" refers to the situation where Japan is spending more money on data and digital technologies than it is receiving or benefiting from.<sup>44</sup> This is perceived as a disadvantage where Japan is heavily reliant on foreign digital technologies and services, leading to an outflow of capital and

<sup>43</sup> We list the main ones: the INPACE project (supporting the EU Digital Partnership with the Republic of Korea, Japan and Singapore and the Trade and Technology Council with India), the IndicoGlobal project (Digital policies and ICT standardisation globally), the INSTAR project (International Standards promotion in implementation globally supporting Europe's Digital Partnerships and the EU-US TTC) and the Digital Partnership in Action Tender.

<sup>44</sup> <https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/news/japans-2024-open-source-promotion-report>

potentially impacting its technological independence and competitiveness. The report suggests that leveraging OSS and embracing it as a public good, is a potential strategy to address this digital deficit and increase digital sovereignty. The report also advocates for software modernization, adoption of cloud and AI technologies, and building common platforms using OSS. While it addresses software development and cybersecurity aspects of digital sovereignty, it does not touch specific areas like Telco cloud-edge, Carbon Neutral AI, or detailed AI applications which are of interest of NexusForum.EU. On the other hand, the report on Japanese Open Source aligns well with the EU strategy for digital sovereignty:

- Both recognize the importance of AI and cloud technologies for digital sovereignty, but recognise the need for human-centric, rather than profit-centric, AI development.
- Both see OSS as a valuable asset for technology development and security.
- Both aim to enhance their digital capabilities and competitiveness on a global scale.

This section briefly illustrates the preliminary findings and activities of NexusForum.EU in the international context, with a specific focus on Japan which was the focus of this first of the project. In the second part of NexusForum.EU a more extensive analysis will be performed, including also the Republic of Korea, where a similar workshop to the one organised in Tokyo is planned in the first half of 2026.

## Conclusions

Deliverable D3.2, “Digital Policy Report – b”, advances on the continuous support by NexusForum.EU to the European computing constituency by monitoring and analyzing the evolving regulatory and policy landscape related to the Cognitive Computing Continuum. Building upon the initial insights from D3.1, this second report offers a more comprehensive understanding of the implications of key regulations and policy initiatives on the scientific and industrial ecosystems. It provides a forward-looking analysis of upcoming developments and proposes a structured approach to align research and innovation priorities across the continuum.

This report's comprehensive analysis has yielded several key findings that have significant implications for EU sovereignty in the Cognitive Computing Continuum. By examining six critical factors and conducting a SWOT analysis, informed by stakeholder engagement, we have identified crucial areas where policy interventions can enhance EU sovereignty. Our research highlights the need for strategic actions to address the challenges and opportunities arising from the Computing Continuum. Additionally, the report expands the project's scope by addressing the role of Open Source Software in the context of digital sovereignty, particularly in the agriculture sector, and by continuing the analysis of the international landscape, with a specific focus on the Japanese ecosystem.

Our comprehensive SWOT analysis has revealed several fundamental gaps in the EU computing continuum, which must be addressed to achieve consolidation and technological sovereignty:

- **Federated Technologies Ecosystem:** Developing a shared ecosystem across edge, cloud, and IoT will enhance resource utilization, collaboration, and digital sovereignty, ultimately improving competitiveness.
- **European Data Strategy:** Implementing a single market for data and Common European Data Spaces will promote innovation, data sovereignty, and market growth.
- **Coordinated Open-Source Strategy:** Overcoming fragmentation and ensuring a sustainable computing ecosystem requires a coordinated approach to open-source maintenance, scalability, and skills development.
- **Unified Digital Infrastructure:** Building a unified, open, and secure digital infrastructure will support AI factories and their integration with High-Performance Computing, fostering innovation across key sectors.
- **Strategic International Cooperation:** Collaborating with like-minded countries, such as Japan, South Korea, and Canada, can strengthen cloud and edge infrastructure and reduce dependence on non-European hyperscalers.
- **EU Semiconductor Strategy:** Addressing supply chain vulnerabilities and supporting SMEs in the Cognitive Computing Continuum requires a new EU semiconductor strategy.
- **Simplified Digital Regulations:** Harmonizing digital regulations will reduce fragmentation, lower compliance costs, and enable a more competitive and innovative Digital Single Market across Cloud, Edge, and IoT.

Raising awareness about complex policy issues is a formidable challenge, particularly when dealing with abstract concepts, technical jargon, and unclear messaging. The NexusForum.EU project has faced this challenge head-on, and our experience highlights the importance of a structured approach to engaging stakeholders and promoting awareness. Initially, our efforts to engage stakeholders were met with limited success, underscoring the difficulty of conveying complex policy issues in an accessible and compelling manner. However, by developing and implementing a methodology to raise awareness and encourage participation in policy

initiatives, we have made significant progress in fostering a more inclusive and proactive policy development process.

The findings and insights presented in D3.2 will serve as a key input for the next phases of the project, with the following planned activities:

- NexusForum.EU will continually update and monitor policies and regulations contributing to a more comprehensive mapping of European initiatives, supporting policy alignment and cross-project collaboration. It will also drive specific mapping and alignment to the NexusForum.EU R&D roadmap of latest policy frameworks and regulations such as the **AI continent action plan**.<sup>45</sup> Additionally, as soon as the **EU Cloud and AI Development Act** is proposed in draft form by the European Commission, it will be promptly included in the analysis to ensure NexusForum.EU remains up-to-date and aligned with the latest regulatory developments.
- The methodology developed for **raising awareness and encouraging participation in policy initiatives** will be actively implemented through targeted outreach, including the organization of public consultations, co-creative workshops, and stakeholder engagement events.
- Building on the SWOT analysis and the identified gaps in the six key factors, the project will continue **to refine and validate policy-related recommendations through structured discussions in the Working Groups**. These recommendations will be further enriched by stakeholder feedback and aligned with the broader goals of EU digital sovereignty and competitiveness.
- The project will **further explore the role of Open Source Software in supporting digital sovereignty**, particularly in key sectors, and will identify opportunities for the NexusForum.EU community to contribute to and benefit from open innovation initiatives.
- Building on the initial insights from the **EU-Japan Digital Week** and the outcomes of the **Japan Workshop and Summit**, the project will continue to explore opportunities for international collaboration, with a view to strengthening cross-border policy alignment and knowledge exchange specially with ROK.

The third and final version of the Digital Policy Report “D3.3, “Digital Policy Report – c”, scheduled for M30, will consolidate the findings from the previous reports and present a comprehensive, strategic overview of the regulatory landscape, policy recommendations, and the project’s contribution to shaping the future of the Cognitive Computing Continuum in Europe.

<sup>45</sup> [https://commission.europa.eu/topics/eu-competitiveness/ai-continent\\_en](https://commission.europa.eu/topics/eu-competitiveness/ai-continent_en)

## References

- [1] NexusForum.EU Consortium, “D3.1 Digital Policy Report - a,” 2024.
- [2] NexusForum.EU Consortium, “D2.2 Research & Innovation Roadmap - b,” 2024.
- [3] European Commission, “Annex I: New initiatives, COM(2025) 45 final - Commission Communication 'Commission work programme 2025',” 2025.

## Annex 1 – EUCloudEdgeIoT.eu Digital policies visualisation

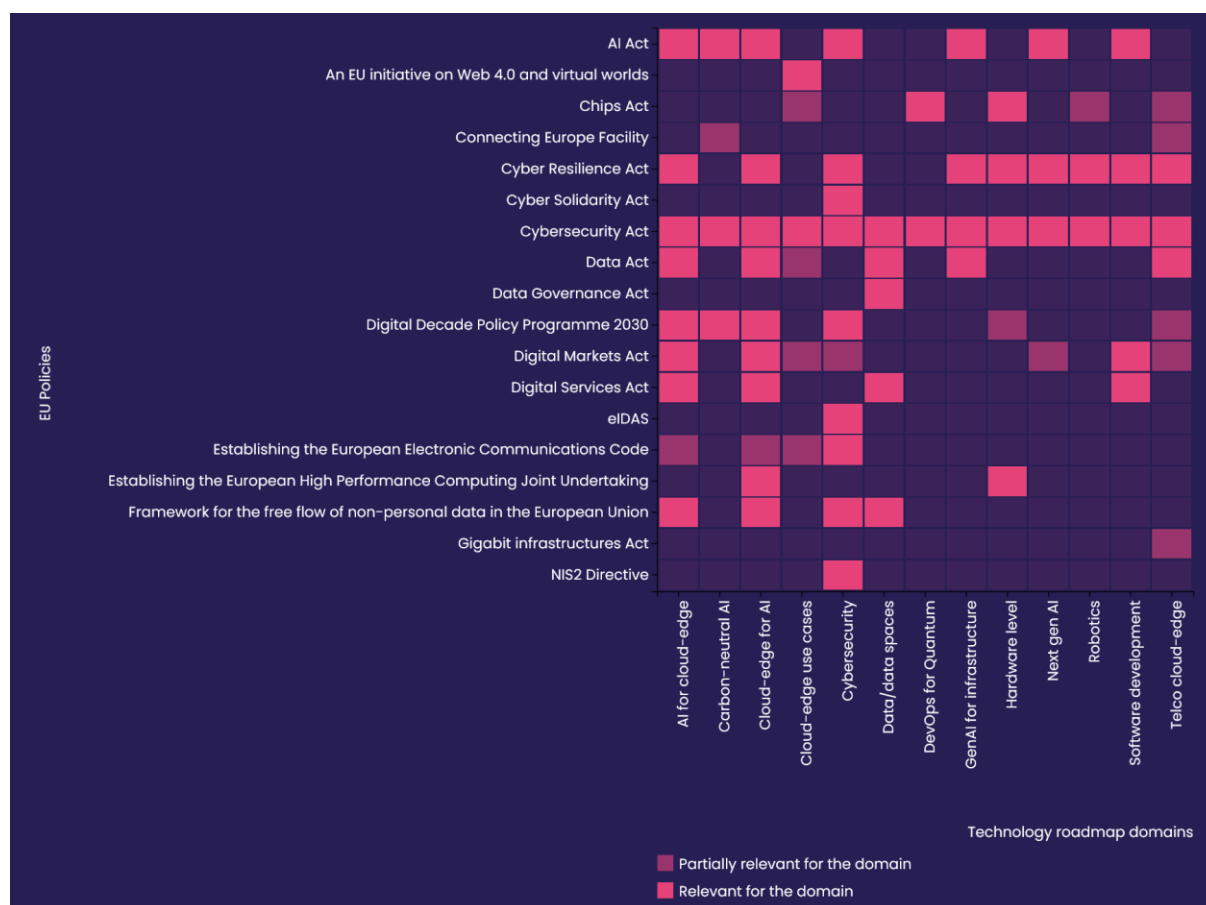


Figure 12 - eucloudedgeiot.eu - Policies and initiatives interactive visualisation in the EUCEI webpage

The following pages contain the descriptive text made available through the interactive visualisation for each of the technology domains vis-à-vis each policy document. At the time of writing, the interactive visualisation is available at: <https://eucloudedgeiot.eu/policies-initiatives/>



	Framework for the free flow of non-personal data in the European Union	Data Act	Cybersecurity Act	Cyber Resilience Act
AI for cloud-edge	<p>The Framework for the Free Flow of Non-Personal Data aims to remove barriers to the movement and storage of non-personal data within the EU. For companies developing AI for cloud-edge technology, this framework enables them to store and process data across borders within the EU without facing national data restrictions, fostering more flexible, interoperable and efficient operations. It also supports innovation by encouraging data sharing and access, which is crucial for AI development. For users, it means that their non-personal data can be used more freely and across different platforms, helping to drive new AI-driven services. The framework also includes safeguards to ensure that concerns related to data sovereignty, such as national security, are respected, providing a balance between free data flow and regulatory protections. For more information, please visit: <a href="https://digital-strategy.ec.europa.eu/en/faqs/business-government-data-sharing-questions-and-answers">https://digital-strategy.ec.europa.eu/en/faqs/business-government-data-sharing-questions-and-answers</a></p>	<p>The EU Data Act aims to improve the accessibility and sharing of data across the EU, enhancing the use of data for innovation while ensuring security and privacy. For companies developing AI for cloud-edge technology, the Data Act mandates that they make certain data generated by their products accessible to third parties under clear conditions, fostering data sharing and interoperability. This could help fuel innovation in AI by making data more available for training and improving algorithms. For users, the Data Act offers greater control over their data, ensuring they can access, share, and even transfer their data across platforms. However, the law also includes provisions to ensure that such data sharing doesn't compromise privacy or security, aligning with broader EU data protection regulations. For more information, please visit: <a href="https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act">https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act</a></p>	<p>The Act enhances the mandate of the European Union Agency for Cybersecurity (ENISA). For companies developing AI for cloud-edge technology, the act mandates that certain critical digital products and services must meet specific cybersecurity standards, ensuring that they are resilient to cyber threats. This also involves a new certification system, which can help companies demonstrate compliance with cybersecurity best practices and build trust in their products. For users, the Cybersecurity Act offers greater assurance that the AI and digital products they use are secure, reducing the risk of cyberattacks. It enhances transparency by requiring companies to disclose their security practices and ensuring that the EU has more centralised and effective cybersecurity governance. For more information, please visit: <a href="https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_3369">https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_3369</a></p>	<p>The Cyber Resilience Act impacts companies developing AI products because it mandates that they integrate robust security measures into their design, ensuring resilience against cyber threats throughout the lifecycle of the product. This includes conducting risk assessments, implementing secure coding practices, and providing clear vulnerability management. For users, the Act offers a higher level of confidence in the security of cloud-edge AI products, as they will be subject to rigorous compliance standards, reducing exposure to cyber risks. In essence, it elevated the security bar for both product creators and end-users across the EU. For more information, please visit: <a href="https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5375">https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5375</a></p>

	Establishing the European High Performance Computing Joint Undertaking	AI Act	Digital Decade Policy Programme 2030	Establishing the European Electronic Communications Code	Digital Services Act
Cloud-edge for AI	<p>This initiative enhances Europe's supercomputing capabilities, providing businesses access to cutting-edge computing power for AI model development and data processing. It ensures compliance with EU data protection laws, offering AI companies secure, sovereign cloud-edge services. By reducing dependency on non-EU providers, the initiative boosts the competitiveness of European AI firms both locally and globally. It also promotes innovation through collaborative research and cost-effective access to high-performance resources. Due to its emphasis on sustainability, it enables businesses to run energy-efficient, large-scale AI applications while lowering operational costs. For more information, please visit: <a href="https://op.europa.eu/en/web/who-is-who/organization/-/organization/corporate-body/EUROHPC">https://op.europa.eu/en/web/who-is-who/organization/-/organization/corporate-body/EUROHPC</a></p>	<p>Depending on its risk classification level, the AI Act imposes specific obligations to which the company has to adhere. Furthermore, the data generated by the AI systems and data used to train AI models needs to respect transparency measures. For more information, you can submit your questions here: <a href="https://aiacthub.eu/">https://aiacthub.eu/</a></p>	<p>EU programme designed to promote innovation and investment in the EU. One of its main objectives is to support the development of comprehensive and sustainable ecosystem of interoperable digital infrastructures, where high performance, edge, cloud, quantum computing, artificial intelligence, data management and network connectivity converge. In concrete terms, the ambition is to reach at least a 75% of cloud computing services, big data or artificial intelligence uptake by European businesses. For more information, please visit: <a href="https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade">https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade</a></p>	<p>The Code supports the enhancement of 5G networks and edge infrastructure, which helps companies develop AI applications that require low latency and high bandwidth. Since it pushes for infrastructure sharing, the code is very relevant for smaller firms looking to leverage AI without needing giant upfront investments in network infrastructure. It also encourages innovation through public-private partnerships, which could foster AI solutions that are more integrated with cloud-edge infrastructure. For more information, please visit: <a href="https://ec.europa.eu/commission/presscorner/detail/en/memo_18_4084">https://ec.europa.eu/commission/presscorner/detail/en/memo_18_4084</a></p>	<p>The Act enforces strict rules around data protection and transparency when deploying AI in the edge, especially in user-sensitive applications. Due to these technologies' reliance on data storage across different locations, it is critical to comply with data sovereignty and content moderation standards. The Act also pushes cloud-edge providers to adopt more rigorous data governance and monitoring framework, since it holds companies accountable for the legal and ethical implications of AI-driven services with the aim of obtaining mechanisms that mitigate risks such as harmful algorithmic outputs or privacy violations. For more information, please visit: <a href="https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers">https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers</a></p>

	Digital Markets Act	Framework for the free flow of non-personal data in the European Union	Data Act	Cybersecurity Act	Cyber Resilience Act
Cloud-edge for AI	<p>If a company developing or using cloud-edge AI solutions is considered as a Gatekeeper under the Digital Markets Act affects, or else is designated as a large platform with significant control over access to users and services - such as major cloud providers or AI-driven platforms - some restrictions may apply. Indeed, these parties must comply with strict obligations to prevent anti-competitive practices, like self-preferencing and restricting third-party access to their services. The Act ensures that smaller companies, including AI startups, can access the same market opportunities, promoting innovation and fair competition. Violating the Digital Markets Act provisions could result in substantial fines, impacting both gatekeepers and users reliant on their services. For more information, please visit: <a href="https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers_en">https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers_en</a></p>	<p>This Regulation aims to eliminate data localization requirements within the EU, promoting the free movement of non-personal data across member states. This framework is particularly relevant for companies developing or using cloud-edge AI technologies, as it enables them to store, process, and transfer non-personal data freely across borders within the EU. By removing restrictions on where non-personal data can be stored or processed, it supports innovation and efficiency, helping businesses scale and enhance their AI solutions. However, companies must still comply with EU data protection laws like the GDPR for personal data, ensuring that data privacy and security standards are maintained. This regulation thus facilitates more seamless data flows, while balancing the need for security and compliance. For more information, please visit: <a href="https://digital-strategy.ec.europa.eu/en/faqs/business-government-data-sharing-questions-and-answers">https://digital-strategy.ec.europa.eu/en/faqs/business-government-data-sharing-questions-and-answers</a></p>	<p>The Data Act is designed to regulate the access, sharing, and use of data across the European Union, particularly focusing on enhancing data portability, availability, and use for innovation. For companies dealing with the development of cloud-edge AI solutions, the Act impacts how data generated or processed by their products can be accessed and shared with third parties. It mandates that data generated by IoT devices, AI systems, and other digital technologies be made accessible to users and businesses, subject to clear terms and conditions, while safeguarding privacy and security. This could influence how AI providers structure their services and data-sharing agreements, ensuring compliance with the rules on data ownership, consent, and transfer. Additionally, it creates a more open data environment, potentially boosting innovation but also requiring strict adherence to data protection standards. For more information, please visit: <a href="https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act">https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act</a></p>	<p>The EU Cybersecurity Act strengthens the EU's overall cybersecurity framework. It establishes the European Cybersecurity Certification Framework, which sets standards for cybersecurity certification across various sectors, including AI and cloud-edge technologies. Companies developing or using AI technology solutions within the EU are impacted by the Act, as they may be required to obtain cybersecurity certifications for their products and services. This ensures that these solutions meet high cybersecurity standards, mitigating risks for users and increasing trust in the technologies. Non-compliance could result in market restrictions and reduced competitiveness in the EU. For more information, please visit: <a href="https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_3369">https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_3369</a></p>	<p>The EU Cyber Resilience Act imposes conditions on European companies developing or using AI for Cloud Edge technologies. Indeed, they must ensure that their products meet specific security requirements, such as secure development practices, timely updates, and risk management processes. Non-compliance could lead to penalties or restrictions in the EU market. Additionally, the act mandates that users and organizations using these technologies must adhere to safety protocols, ensuring robust protection against cyber threats. In practice, this drives both innovation and accountability in the security of AI and cloud-edge solutions. For more information, please visit: <a href="https://www.pwc.ch/en/insights/regulation/understanding-the-eu-cyber-resilience-act.html">https://www.pwc.ch/en/insights/regulation/understanding-the-eu-cyber-resilience-act.html</a></p>

	AI Act	Data Act	Cybersecurity Act	Cyber Resilience Act
GenAI for infrastructure	Depending on its risk classification level, the AI Act imposes specific obligations to which the company has to adhere. Furthermore, the data generated by the AI systems and data used to train AI models needs to respect transparency measures. For more information, you can submit your questions here: <a href="https://aiacthub.eu/">https://aiacthub.eu/</a>	The Data Act is a far-reaching Regulation which covers the wider European data ecosystem, regulating the exchanges of data as well of the protection and exchange of data in specific contexts. The regulation requires actors in the digital ecosystem to make certain types of data available for third parties, thus contributing to the data economy and reducing the barriers for consumers to switch between different data processing services. The regulation also outlines provisions for the protection of trade secrets and does not reduce the scope of application of the General Data Protection Regulation. Given its cross-cutting domain of application, the Data Act is of relevance to AI implementations managing and generating data and the exchange of data. For more information, please visit: <a href="https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act">https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act</a>	On top of strengthening the EU Agency for cybersecurity (ENISA), the EU Cybersecurity Act “introduces an EU-wide cybersecurity certification framework for ICT products, services and processes”, this means that the measures defined in the act are cross-cutting and apply on a wide range of digital goods and services. Cybersecurity measures outlined in the Act may apply to some implementations of Generative AI for infrastructure. Information and updates on the Cybersecurity Certification on the ENISA website: <a href="https://certification.enisa.europa.eu/index_en">https://certification.enisa.europa.eu/index_en</a>	The Cyber Resilience Act refers to products with digital elements entering the market, and aims to ensure the cybersecurity of all components within the supply chain. The specific requirements vary depending on the classification of the product, with particular reference to the level of risk. This is particularly relevant in the field of Generative AI for infrastructure, as AI components may be considered high-risk (Art. 12), and are therefore subject to specific requirements. For more information, please visit: <a href="https://www.pwc.ch/en/insights/regulation/understanding-the-eu-cyber-resilience-act.html">https://www.pwc.ch/en/insights/regulation/understanding-the-eu-cyber-resilience-act.html</a>

	Cyber Solidarity Act	Connecting Europe Facility	Digital Decade Policy Programme 2030	Digital Markets Act
Telco cloud-edge		<p>The Facility impacts telco cloud edge technologies by providing funding to support the deployment of high-performance digital infrastructure across Europe. Through the Facility, European firms developing this kind of technologies can access grants for projects that enhance connectivity, improve digital services, and expand broadband networks, particularly in underserved remote areas. For telco providers, the funding can help scale edge data centres and 5G infrastructure, fostering innovation in low-latency services. By improving the backbone for cloud-edge services, the Facility enables businesses to deliver faster, more reliable services to end-users. This creates opportunities for both providers and consumers, with European companies better positioned in the competitive global digital landscape. For more information, please visit: <a href="https://hadea.ec.europa.eu/calls-tenders_en">https://hadea.ec.europa.eu/calls-tenders_en</a> For more information, you can ask your questions here: <a href="https://hadea.ec.europa.eu/contact-form_en">https://hadea.ec.europa.eu/contact-form_en</a></p>	<p>EU programme designed to promote innovation and investment in the EU. One of its main objectives is to support the development of comprehensive and sustainable ecosystem of interoperable digital infrastructures, where high performance, edge, cloud, quantum computing, artificial intelligence, data management and network connectivity converge. In concrete terms, the ambition is to reach at least a 75% of cloud computing services, big data or artificial intelligence uptake by European businesses. For more information, please visit: <a href="https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade">https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade</a></p>	<p>For European companies developing telco cloud-edge solutions, the Digital Markets Act could impose stricter rules on gatekeeper platforms, fostering a more level playing field and encouraging innovation. It aims at the prevention of market dominance by few players, allowing smaller firms in the telecom sector to compete more efficiently. Users of these technologies may benefit from more competitive pricing and improved service offering as a result of increased market fairness. For more information, please visit: <a href="https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers_en">https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers_en</a></p>

	Chips Act	Data Act	Cybersecurity Act
<b>Telco cloud-edge</b>	<p>Companies developing telco cloud-edge solutions are impacted by the Chips Act in terms of funding and incentives to build and scale semiconductor manufacturing within Europe, which in return enhances supply chain for critical hardware. This can lead to more reliable and cost-effective components for telco infrastructures. Users of cloud-edge technologies can benefit from improved hardware availability, performance and security, as European-made advanced chips are prioritized. For more information, please visit: <a href="https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_4519">https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_4519</a></p>	<p>The Data Act could amplify data sharing across borders and sectors, creating new opportunities for innovation and service offerings. This would benefit companies developing telco cloud-edge solutions, while also increasing the level of transparency of data usage, which could help smaller market players compete with larger players. On the other hand, users of these technologies would likely experience more accessible, secure, and fair data practices, enhancing trust in services, and granting them more freedom of choice when it comes to data storage. For more information, please visit: <a href="https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act">https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act</a></p>	<p>The Act strengthens the EU's cybersecurity framework, setting clear cybersecurity standards that companies developing telco cloud-edge solutions must meet, ensuring greater security and trust in their offerings. The Act also mandates that critical infrastructure, including telecom networks, implement robust cybersecurity measures, which could drive higher compliance costs but also offer opportunities to differentiate through secure services. Users of these technologies benefit from improved protection against cyber threats and greater confidence in the reliability of services. For more information, please visit: <a href="https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_3369">https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_3369</a></p>



	An EU initiative on Web 4.0 and virtual worlds	Establishing the European Electronic Communications Code	Digital Markets Act	Chips Act	Data Act	Cybersecurity Act
Cloud-edge use cases	<p>The initiative aims to advance the next generation of the internet, creating immersive, decentralised environments that integrate AI, blockchain, and advanced cloud-edge computing. For businesses using or producing cloud-edge AI solutions, this offers new opportunities to leverage virtual worlds for innovative products, services and customer engagement. The initiative encourages collaboration between tech companies to develop scalable and secure virtual platforms, enhancing cross-sector use cases like e-commerce, healthcare and education. It also fosters data sovereignty and privacy by ensuring European regulations govern these virtual environments. Investing in Web 4.0, companies can access cutting-edge infrastructure and expand their capabilities in real-time, decentralised and interactive AI applications. For more information, please visit: <a href="https://ec.europa.eu/commission/presscorner/api/files/document/en/qanda_23_3719/QANDA_23_3719_EN.pdf">https://ec.europa.eu/commission/presscorner/api/files/document/en/qanda_23_3719/QANDA_23_3719_EN.pdf</a></p>	<p>The Code directly impacts the development of network infrastructure, regulation, and service delivery models that are essential to edge computing. The Code promotes the rollout of high-speed broadband such as fiber-optic networks and next-generation technologies such as 5G, which are crucial for cloud-edge operations. Given the support to enhancing broadband infrastructure and accelerating 5G deployment, this EU instrument can be beneficial for use cases like autonomous vehicles, IoT (i.e. smart cities) and real-time data processing where latency is of critical importance. For more information, please visit: <a href="https://ec.europa.eu/commission/presscorner/detail/en/memo_18_4084">https://ec.europa.eu/commission/presscorner/detail/en/memo_18_4084</a></p>	<p>For cloud-edge use cases, the Digital Markets Act implies that smaller EU companies developing new services are less likely to face unfair advantages from dominant platform providers. The act helps create a more level playing field, fostering innovation by allowing emerging players to compete on more equal terms. Companies in sectors like fintech, retail, or media can particularly benefit as the act ensures they have the opportunity to scale up their cloud-edge solutions without being stifled by market concentration. For more information, please visit: <a href="https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers_en">https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers_en</a></p>	<p>The Chips Act is significant for cloud and edge computing as it directly impacts the hardware on which these services are built. Indeed, the Act focuses on increasing semiconductor production within the EU and ensuring access to cutting-edge chips. By supporting local chip manufacturing, the act can reduce supply chain dependencies and boost innovation in specialised processing power required for edge computing. Companies developing use cases in AI, autonomous vehicles, supercomputing, defence and space capabilities or smart cities can particularly benefit from this, as localised access to high performance chips can lead to faster, more efficient edge-based computations. For more information, please visit: <a href="https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_4519">https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_4519</a></p>	<p>The Data Act influences cloud-edge use cases put forward by third parties because it aims at ensuring interoperability between different platforms and services. It also encourages innovation by promoting the use of data across borders, driving new business models. Firms developing solutions for industries such as IoT, agriculture, or manufacturing stand to benefit as the Act encourages the flow of real-time data for edge analytics and decision-making. For more information, please visit: <a href="https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act">https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act</a></p>	<p>The Cybersecurity Act establishes requirements for cybersecurity certification, which directly impacts cloud and edge computing use cases, especially for EU-based companies. Cloud and edge providers offering services within the EU must adhere to robust security standards, ensuring that their infrastructures are resilient against cyber threats. This is relevant for industries like healthcare, finance, and critical infrastructure that require high levels of trust and data protection. Companies offering such solutions benefit from the Act by gaining trust in the marketplace through recognized certifications, which enhances their appeal to EU consumers who prioritise security and compliance. For more information, please visit: <a href="https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_3369">https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_3369</a></p>

	AI Act	Connecting Europe Facility	Digital Decade Policy Programme 2030	Cybersecurity Act
Carbon-neutral AI	<p>Depending on its risk classification level, the AI Act imposes specific obligations to which the company has to adhere. Furthermore, the data generated by the AI systems and data used to train AI models needs to respect transparency measures. For more information, you can submit your questions here: <a href="https://aiacthub.eu/">https://aiacthub.eu/</a></p>	<p>The Regulation establishing the “Connecting Europe Facility” does not exclusively focus on the European digital ecosystem but rather looks at trans-European networks in the transport, energy and digital sectors. This means that, while virtually having the potential to touch upon all the roadmap technologies, it can be found to indirectly address Telco cloud-edge, integration with 5G and 6G and Carbon-neutral edge/AI, Carbon Neutral Edge Intelligence, considering in particular its energy- and environment- related objectives.</p> <p>The Regulation defines a key funding scheme which directly targets the digital ecosystem, making grant opportunities available for eligible initiatives. More information on calls for proposals: <a href="https://hadea.ec.europa.eu/programmes/connecting-europe-facility_en">https://hadea.ec.europa.eu/programmes/connecting-europe-facility_en</a></p>	<p>According to Article 3.1 (e), The Decision aims at developing a comprehensive and sustainable ecosystem of interoperable digital infrastructures, where high performance, edge, cloud, quantum computing, artificial intelligence, data management and network connectivity work in convergence, to promote their uptake by businesses in the Union, and to create opportunities for growth and jobs through research, development and innovation, and ensuring that the Union has a competitive, secure and sustainable data cloud infrastructure in place, with high security and privacy standards and complying with the Union data protection rules. The scope of the Decision is quite wide-encompassing, and as such touches upon several of the technologies examined in the roadmap, with particular reference to AI for Cloud, Cloud for AI, Carbon-neutral edge/AI, Carbon Neutral Edge Intelligence, Cybersecurity and indirectly addresses Telco cloud-edge, integration with 5G and 6G and Hardware level (HPC – RISC-V). For more information, please visit: <a href="https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade">https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade</a></p>	<p>On top of strengthening the EU Agency for cybersecurity (ENISA), the EU Cybersecurity Act “introduces an EU-wide cybersecurity certification framework for ICT products, services and processes” , this means that the measures defined in the act are cross-cutting and apply on a wide range of digital goods and services. Cybersecurity measures outlined in the Act may apply to some Artificial Intelligence implementations.</p> <p>Information and updates on the Cybersecurity Certification on the ENISA website: <a href="https://certification.enisa.europa.eu/index_en">https://certification.enisa.europa.eu/index_en</a></p>

	Establishing the European High Performance Computing Joint Undertaking	Digital Decade Policy Programme 2030	Chips Act	Cybersecurity Act	Cyber Resilience Act
Hardware level	<p>EuroHPC JU provides companies with access to advanced high-performance computing (HPC) resources enabling them to perform complex simulations, computational modelling, and data-intensive analytics more efficiently. This can drive innovation and enhance their competitiveness, being able to develop cutting-edge solutions, optimize production processes, and reduce time-to-market for new products. It also offers funding opportunities and support for SMEs to integrate HPC into their operations. In its projects, EuroHPC JU places a strong emphasis on sustainability and ethical issues. Businesses should conduct their operations in accordance with these guidelines to make sure that their efforts support the EU's overarching objectives of ethical innovation and sustainability (such as low-power micro-processing components). For additional details: Get in touch with Contact - EuroHPC JU</p>	<p>The Digital Decade Policy Programme 2030's goal is to transform Europe's digital landscape by setting ambitious targets for digital infrastructure; this includes widespread gigabit connectivity and advanced semiconductors, driving demand for efficient hardware solutions. It focuses on sustainable and secure digital infrastructures, requiring hardware manufacturers to comply with strict security regulations. For example, one of the digital goals is for the Union to produce at least 20% of the world's value of advanced semiconductors in compliance with Union law on environmental sustainability. The programme drives innovation through multi-country projects and highlights the need for digital skills across the workforce. In this context, SMEs play a crucial role, with goals for over 90% to achieve basic digital intensity and providing opportunities for funding and collaboration on innovative projects. For more information, please visit: <a href="https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade">https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade</a></p>	<p>The European Chips Act has several key goals aimed at strengthening Europe's position in the semiconductor industry; some of these are: increasing production capacity to 20% of the global market by 2030, enhancing innovation in chip design and manufacturing, ensuring supply chain resilience, and supporting start-ups and SMEs through improved financing access. The Act introduces measures to streamline the process and fast-track procedures for semiconductor manufacturing facilities, helping companies to bring new technologies to market faster. On the other hand, the creation of a European Chips Infrastructure Consortium encourages collaboration between public and private sectors, fostering innovation and technological advancement. You can find more information here: European Chips Act - Questions and Answers</p>	<p>1. The European Cybersecurity Act mainly focuses on establishing a framework for cybersecurity certification of ICT products, services, and processes. This framework will enable the assurance that hardware products meet specific security standards, at different levels depending on the risk of its use. The compliance with this certification will facilitate the access to the European Market as well as gain the consumers' trust. Furthermore, the act aims to achieve a consistent approach to cybersecurity for hardware products. For further details visit European Chips Act - Questions and Answers or contact ENISA <a href="mailto:info@enisa.europa.eu">info@enisa.europa.eu</a></p>	<p>The European Cyber Resilience Act (CRA) has a significant impact at hardware level as it sets mandatory cybersecurity standards for products with digital elements sold in the EU. It looks out for products to be secure throughout their lifecycle. Manufacturers must conduct conformity assessments to ensure their products meet the CRA's standards and are also required to report any actively exploited vulnerabilities to the European Union Agency for Cybersecurity (ENISA). For more information: Cyber Resilience Act - Questions and Answers or contact ENISA <a href="mailto:info@enisa.europa.eu">info@enisa.europa.eu</a></p>

	AI Act	Digital Services Act	Digital Markets Act	Cybersecurity Act	Cyber Resilience Act
Software development	<p>The AI Act establishes strict regulations for AI systems in the EU, impacting software development by enforcing risk-based classification, with high-risk AI systems requiring compliance with risk assessments, data governance, and human oversight. Certain AI practices, like manipulative AI and social scoring, are banned, while transparency and accountability obligations require clear documentation and user disclosures. The Act also supports innovation through regulatory sandboxes for AI testing. Non-compliance can lead to fines of up to €35 million or 7% of global turnover, making adherence essential for AI developers operating in Europe. For more information, you can submit your questions here: <a href="https://aiacthub.eu/">https://aiacthub.eu/</a></p>	<p>The Digital Services Act (DSA) impacts software development by enforcing stricter content moderation, requiring platforms to detect and remove illegal content while ensuring transparency in moderation decisions. It also limits targeted advertising, particularly for minors and sensitive data, affecting ad-tech development. Algorithmic transparency is mandated, giving users more control over personalized content. Developers must also implement business user traceability for online marketplaces to verify seller identities, enhancing trust. These regulations push software companies to build more responsible, transparent, and secure digital services. Ask your questions here: <a href="https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers">https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers</a></p>	<p>The Digital Markets Act (DMA) ensures fair competition in the EU digital sector by imposing obligations on gatekeepers—large tech companies controlling key digital services. It mandates interoperability, allowing third-party developers to integrate with dominant platforms, and prohibits self-preferencing, ensuring fair treatment of competing services. The DMA also enforces data portability, requiring platforms to enable users to transfer their data, and access to platform data, allowing businesses to leverage user-generated data for innovation. These measures create a more competitive and transparent software development landscape. For more information, you can ask your questions here: <a href="https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers_en">https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers_en</a></p>	<p>The Cybersecurity Act establishes a EU-wide cybersecurity certification framework, requiring software developers to align with standardised security measures. It defines three assurance levels (basic, substantial, high), pushing developers to implement appropriate security measures. The Act promotes security by design and default, ensuring software is secure from the outset, and mandates vulnerability handling and disclosure, requiring continuous monitoring, patching, and transparency in security updates. For more information, you can ask your questions here: <a href="https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_3369">https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_3369</a></p>	<p>The Cyber Resilience Act (CRA) enforces strict cybersecurity requirements for digital products in the EU, directly impacting software development. Developers must implement state-of-the-art security measures, ensure vulnerability management and timely updates, and comply with conformity assessments to obtain CE marking for market access. The Act also mandates transparent documentation of security measures for regulatory and consumer access. Non-compliance risks fines and market restrictions, making cybersecurity a critical aspect of software development for the EU market. For more information: Cyber Resilience Act - Questions and Answers or contact ENISA <a href="mailto:info@enisa.europa.eu">info@enisa.europa.eu</a></p>

	Cyber Solidarity Act	eIDAS	AI Act	Digital Decade Policy Programme 2030	Establishing the European Electronic Communications Code
Cybersecurity	<p>By establishing a pan-European infrastructure of Security Operations Centres (European Cyber Shield), the Act seeks to enhance real-time detection and situational awareness of cyber threats. This initiative mandates that European companies, especially those operating critical infrastructures, align their technologies with standardized detection and response protocols. Consequently, businesses are encouraged to adopt advanced cybersecurity measures and participate in information-sharing frameworks, thereby strengthening their resilience against cyber threats and contributing to a more secure digital ecosystem across the EU. For more information, you can ask your questions here: <a href="https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda_23_2244/qanda_23_2244_en.pdf">https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda_23_2244/qanda_23_2244_en.pdf</a></p>	<p>eIDAS Regulation establishes a comprehensive framework for electronic identification and trust services across the European Union. By standardizing electronic identification and authentication processes, it enhances the security of digital transactions for European companies. The regulation mandates rigorous requirements for electronic signatures, seals, and timestamps, ensuring data integrity and authenticity. Consequently, businesses are encouraged to adopt secure electronic identification systems and trust services, thereby strengthening their cybersecurity posture and facilitating trusted cross-border digital interactions. For more information, visit this page: <a href="https://digital-strategy.ec.europa.eu/en/policies/learn-about-eidas">https://digital-strategy.ec.europa.eu/en/policies/learn-about-eidas</a></p>	<p>The Artificial Intelligence Act establishes harmonized rules for the development, placement on the market, and use of AI systems within the European Union. By categorizing AI applications based on risk levels, it mandates stringent security requirements for high-risk AI technologies, ensuring that European companies develop and deploy AI solutions that are secure and trustworthy. This regulatory framework compels businesses to implement robust cybersecurity measures, conduct thorough risk assessments, and ensure transparency in AI operations, thereby enhancing the overall security and trustworthiness of AI technologies used by European companies. For more information, you can submit your questions here: <a href="https://aiacthub.eu/">https://aiacthub.eu/</a></p>	<p>The Digital Decade Policy Programme 2030 outlines the European Union's vision for digital transformation by 2030, emphasizing the importance of robust cybersecurity measures. It sets specific targets for digital skills, infrastructure, and public services, encouraging European companies to invest in secure digital infrastructures and adopt best practices to protect against cyber threats. By promoting the development of secure digital technologies and services, the programme aims to enhance the overall cybersecurity posture of businesses operating within the EU. For more information: <a href="https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade">https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade</a></p>	<p>European Electronic Communications Code (EECC), establishes a comprehensive regulatory framework for electronic communications within the European Union. It emphasizes the security and integrity of public electronic communications networks and services. The directive mandates that providers implement appropriate technical and organizational measures to manage risks posed to the security of networks and services, ensuring a level of security appropriate to the risk presented. This includes measures to prevent and minimize the impact of security incidents on users and interconnected networks. By enforcing these requirements, the EECC enhances the cybersecurity posture of European companies operating in the electronic communications sector, ensuring the resilience and reliability of their services. Ask your questions here: <a href="https://ec.europa.eu/commission/presscorner/detail/en/memo_18_4084">https://ec.europa.eu/commission/presscorner/detail/en/memo_18_4084</a></p>

	Digital Markets Act	Framework for the free flow of non-personal data in the European Union	NIS 2	Cybersecurity Act	Cyber Resilience Act
Cybersecurity	<p>The Digital Markets Act aims to ensure fair and contestable markets in the digital sector by imposing obligations on designated "gatekeeper" platforms. While its primary focus is on promoting competition, the regulation indirectly impacts cybersecurity by requiring these gatekeepers to implement measures that prevent unauthorized access and ensure the integrity of their services. This includes obligations to allow interoperability with third-party services in a secure manner and to provide users with effective control over their data. Consequently, European companies interacting with these platforms can expect enhanced security measures, reducing potential vulnerabilities and contributing to a safer digital ecosystem. For more information, you can ask your questions here: <a href="https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers_en">https://digital-markets-act.ec.europa.eu/about-dma/questions-and-answers_en</a></p>	<p>This Regulation establishes a framework for the free flow of non-personal data within the European Union. By prohibiting data localization requirements, except when justified on grounds of public security, it enables European companies to store and process non-personal data across borders, enhancing operational flexibility and efficiency. The regulation encourages the development of self-regulatory codes of conduct to facilitate data portability and minimize vendor lock-in, promoting a competitive and secure data economy. This approach ensures that businesses can implement robust cybersecurity measures consistently across the EU, fostering a more resilient digital environment. For more information, you can ask your questions here: <a href="https://digital-strategy.ec.europa.eu/en/faqs/business-government-data-sharing-questions-and-answers">https://digital-strategy.ec.europa.eu/en/faqs/business-government-data-sharing-questions-and-answers</a></p>	<p>The NIS2 Directive establishes a unified legal framework to uphold cybersecurity across 18 critical sectors within the European Union. It mandates that both "essential" and "important" entities implement appropriate technical and organizational measures to manage cybersecurity risks, conduct regular risk assessments, and report significant incidents to relevant authorities. The directive also emphasizes the accountability of management bodies, introducing potential personal liability for non-compliance. By enforcing these requirements, the NIS2 Directive enhances the cybersecurity posture of European companies, ensuring the resilience and reliability of their services. For more information: <a href="https://digital-strategy.ec.europa.eu/en/policies/nis2-directive">https://digital-strategy.ec.europa.eu/en/policies/nis2-directive</a></p>	<p>The <b>Cybersecurity Act</b> enhances the role of the European Union Agency for Cybersecurity (ENISA) and establishes a comprehensive framework for cybersecurity certification of information and communications technology (ICT) products, services, and processes. By providing a standardized approach to cybersecurity certification, the Act aims to increase trust and security in digital products and services across the EU. European companies benefit from clear guidelines and certification schemes, enabling them to demonstrate the cybersecurity robustness of their offerings, thereby enhancing their competitiveness and ensuring compliance with EU-wide security standards. For more information, you can ask your questions here: <a href="https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_3369">https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_3369</a></p>	<p>The Cyber Resilience Act establishes comprehensive cybersecurity requirements for products with digital elements within the European Union. It mandates that manufacturers design, develop, and maintain these products with robust cybersecurity measures throughout their lifecycle. This includes ensuring protection against unauthorized access, reducing vulnerabilities, and providing security updates. By enforcing these standards, the Act enhances the cybersecurity posture of European companies, ensuring that digital products are resilient against cyber threats and fostering trust among consumers. For more information: Cyber Resilience Act - Questions and Answers or contact <a href="mailto:ENISA.info@enisa.europa.eu">ENISA.info@enisa.europa.eu</a></p>



	AI Act	Digital Markets Act	Cybersecurity Act	Cyber Resilience Act
Next gen AI	<p>Depending on its risk classification level, the AI Act imposes specific obligations to which the company has to adhere. Furthermore, the data generated by the AI systems and data used to train AI models needs to respect transparency measures. For more information, you can submit your questions here: <a href="https://aiacthub.eu/">https://aiacthub.eu/</a></p>	<p>The digital Markets Act is aimed at guaranteeing a competitive and fair digital sector. The act lays out provisions to help smaller providers of digital services operate in the digital market. The act sets out to achieve this by defining obligations for ‘gatekeepers’ (i.e., particularly large service providers, as defined in Article 3) to reduce the obstacles posed to other actors attempting to access the market. Summary of the main points of the act: <a href="https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4622237">https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4622237</a></p>	<p>On top of strengthening the EU Agency for cybersecurity (ENISA), the EU Cybersecurity Act “introduces an EU-wide cybersecurity certification framework for ICT products, services and processes” , this means that the measures defined in the act are cross-cutting and apply on a wide range of digital goods and services. Cybersecurity measures outlined in the Act may apply to some Artificial Intelligence implementations. Information and updates on the Cybersecurity Certification on the ENISA website: <a href="https://certification.enisa.europa.eu/index_en">https://certification.enisa.europa.eu/index_en</a></p>	<p>The Cyber Resilience Act refers to products with digital elements entering the market, and aims to ensure the cybersecurity of all components within the supply chain. The specific requirements vary depending on the classification of the product. This is potentially very relevant for Next gen AI, as products using future evolutions of the technology may be classified as ‘high-risk’ depending on their field of application. <a href="https://www.pwc.ch/en/insights/regulation/understanding-the-eu-cyber-resilience-act.html">https://www.pwc.ch/en/insights/regulation/understanding-the-eu-cyber-resilience-act.html</a></p>