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

The Cognitive Computing Continuum

Policy Landscape: EU and International Comparisons

Dr Andrew A. Adams
Prof Kiyoshi Murata
(CBIE, Meiji University, Japan)
Enrique Areizaga Sanchez (Tecnalia, Spain)
Francesco Panella (Martel Innovate, Switzerland)

Background

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

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

The EU already has strong links with the countries studied. Canada, Japan, Republic of Korea and New Zealand have all associated with Horizon Europe as global partners. Digital partnership agreements are in place with Japan and Republic of Korea. Trade links (including digital) between the EU and Canada are strong enough that some have even begun discussing whether Canada might somehow join the EU. The 2026 new trade agreement between India and the EU provides a basis for further trade developments, including digital links, as does the recently mostly completed EU-Mercosur agreement (no Mercosur countries were studied in this project due to resource constraints).

Despite these shared concerns about over-reliance on US hyperscalers (and exposure to US foreign policy interference in national affairs via these dependencies), and the developing links with the EU, these non-EU countries are wary of replacing a US hegemon with an EU one. Thus, the NexusForum.EU policy proposals, which are solidly aligned with the already developing EU policies in areas such as Open Source Software (OSS), provide a strong opportunity to develop not just a "fortress EU" in digital sovereignty, but a much larger area of pooled digital sovereignty with strong strength in depth and strength in breadth against internal backsliding on rule of law and treaty arrangements, but also providing capacity and economies of scale to compete with China and the US.

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

Policy Areas Compatibility Review

Cloud-Edge-IoT Policy

The European Union has several policies which apply to the cloud, edge and Internet of Things domains. This includes high-level policies touching upon the wider digital ecosystem, including flagship strategies such as the *Digital Decade Policy Programme 2030* [2], outlining the policy plan and priorities, the *Competitiveness compass* [3], outlining key areas of intervention to support European capacity to compete in a rapidly evolving global context. From a legislative perspective, as anticipated in the introductory paragraph of this chapter, the European Union has a comprehensive set of policies in place to regulate how the European digital ecosystem works. This includes, for instance, flagship policies on safety and cybersecurity such as the *Cyber Resilience Act* [4], the *Cybersecurity Act* [5] and the *Digital Services Act* [6] ensuring from different perspectives that digitally enabled products and services made available in the European Union provide a good level of security and safety to the end-users. The European legislative corpus also includes provisions to ensure the correct functioning of the markets, with specific reference to measures on market competition, via the *Digital Markets Act* [7]: this Regulation is particularly relevant for cloud services, as the provisions to support a fair competition in the market, have direct implications for the cloud ecosystem. Additionally, the European Union has specific regulations in place to define how data can be collected, transferred, stored and reused, which is particularly relevant for the three technology domains explored in this paragraph, with the key legislation on the matter being the *Data Act* [8] and the *Data Governance Act* [9], regulating -from different perspectives- non-personal data exchanges and aimed at supporting a competitive data market ant to establish conditions for the reuse of protected data, the *General Data Protection Regulation* [10], ensuring that a high level of protection of personal data is guaranteed for users located in the European Union. The coming\ months are expected to bring substantial evolutions to the European Union's strategy and regulatory landscape of the digital ecosystem, with particularly high expectations on simplification efforts, aimed at fostering the Bloc's competitiveness.
The Gaia-X initiative represents a pivotal effort by the EU to enhance digital sovereignty through the definition and implementation of federated cloud service protocols. Managed by the Brussels-based non-profit Gaia-X AISBL, the project has been subject to critique—most notably by Adler-Nissen & Eggeling [11]—for the involvement of US hyperscalers such as AWS, Microsoft, and Google in its Working Groups. While official policy states that only EU-based organizations can influence governance, membership continues to include the European subsidiaries of Microsoft, Google Cloud, and Huawei. Although it began as a Franco-German venture, Gaia-X has evolved into a global initiative with members from all countries examined in this project.

In a significant shift, non-European members (DSA Japan, IDRI RoK, and Digital Trust Canada) have recently been elected to the voter group of the Policy Rules Committee (PRC). The PRC's development of the Gaia-X Labels scheme has significantly shaped the EU's "Cloud Sovereignty Framework" [12]. This framework recently culminated in a tender allowing EU institutions and agencies to procure sovereign cloud services for up to €180 million over six years. The successful European bidders include Post Telecom (partnering with CleverCloud and OVHcloud), STACKIT, Scaleway, and Proximus (partnering with S3NS [a joint venture between Thales and Google Cloud],Clarence, and Mistral).

Concerns about the processing of public sector data, particularly sensitive (e.g. national security, law enforcement, government finance) and PII (Personally Identifiable Information) on citizens/residents, are widespread, not just in the countries studied but worldwide (see the

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

UN's Department of Economic and Social Affairs site on National Cloud Strategies for a compendium of many of these policies).

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

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

Artificial Intelligence Research, Innovation and Promotion Policy

The EU AI Office is already engaged with multiple overseas AI Safety Institutes, or equivalent [13]. This includes Japan and Republic of Korea as well as the UK and Australia. The recently expanded trade agreement between the EU and India also includes enhanced cooperation on ensuring the human-centred development of AI. The digital partnership with the Republic of Korea and recent moves in Korea to stress trustworthy AI development, provides a grounding for cooperation to be enhanced in this area. The growing partnership with Canada, which also has an AI Safety Institute, should also provide a solid basis for cooperation. New Zealand lags far behind in this area with no publicly funded AI Safety Institute, only an NPO.

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

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

Semiconductor Design/Production Policy

EU cooperation with Japan and Republic of Korea on semiconductor design and fabrication is already in place in research and innovation. In addition, the EU is “committed to developing a dedicated programme that will facilitate talent exchanges and foster semiconductor skills among students and young professionals” with India [13]. Canada and New Zealand lack significant policies on semiconductor infrastructure. There is an opportunity to expand existing bi-lateral cooperation efforts to multi-lateral, and potentially an opportunity to engage Canada in these with some Canadian voices raising concern about the lack of a semiconductor policy in this area.

A focus on the open RISC-V and related architectures between the EU and these other countries could provide a solid knowledge base for chip and firmware design expertise, while joint funding of fabrication facilities gradually expanding to multiple countries could help address the current concerning bottleneck of Taiwanese manufacturing dominance (deeply worrying given the potential for a Chinese invasion of Taiwan).

Data Spaces Policy

Japan is one of the countries leading the development of Data Spaces, with its Data-EX group now also a member of the Gaia-X grouping. The Data-EX focus on open protocols and FLOSS (Free, Libre and Open Source Software) implementations is very much in tune with EU moves in this area and with the NexusForum.EU R&I roadmap. Korean sectoral integration of data sharing may provide a useful partner in developing data space policies targeted to different sectors (health, education, industry) while the open protocols and infrastructure of the Japanese and EU collaboration could provide a drop-in replacement for the proprietary systems currently in use. India, Canada and New Zealand currently have little involvement in this area, which may be an opportunity for a ground-floor adoption push for the open approach being jointly developed by the EU and Japan, providing a commercial opportunity for Japanese and EU providers as well as cementing pooled digital sovereignty amid the shared approach to data protection of Canada and New Zealand (which both have GDPR adequacy as do Japan and the Republic of Korea). Concerns around the details of India’s current data protection regime [14] are not necessarily a major barrier here, but a solid assessment of compatibility would be worthwhile, perhaps as a Horizon Europe project call seeking to provide a knowledge base on compatibilities and inconsistencies with a wider range of countries with whom digital trade is growing.

The European Union’s common policy organisation on data spaces stems from the 2020 *European Strategy for Data* [15], which laid basis for the Data Act [8] and harmonised the governance of Common European Data Spaces. Currently Common European Data Spaces [16] exist for agriculture, cultural heritage, energy, finance, environmental sustainability, health, manufacturing, language, media, mobility as well as data spaces dedicated to public administrations, research and innovation, skills and tourism.

Smart City Policy

All of the countries studied had invested in smart city pilots and developments, with New Zealand being the weakest here. Further large scale investments in the Republic of Korea and

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

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

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

At an EU level, the smart cities strategy revolves around several lines of action and policy documents. The latest Commission Communication directly targeting Smart Cities is the 2025 Communication 'An EU Agenda for Cities: Driving Growth and Prosperity' [17], which identifies specific tools and actions including the Smart Cities Marketplace, the Horizon Europe-funded EU Mission on Climate-Neutral and Smart Cities [18], aligning to the United Nations's Sustainable Development Goal 11 'Make cities and human settlements inclusive, safe, resilient and sustainable', translated to the European context via the Joint Research Centre's European Handbook for SDG Voluntary Local Reviews. Additionally, the Citiverse European Digital Infrastructure Consortium (EDIC) has been established [19], with an aim to foster an ecosystem of digital solutions and services, leveraging in particular, data, digital twins, artificial intelligence, augmented/virtual reality towards improving urban living and sustainability. These objectives also interact with the EU Local Digital Twins Toolbox: a flagship initiative of the European Commission aimed at providing a 'modular, standards-based suite of tools designed to help cities and communities across Europe simulate, analyse, and plan urban environments more effectively' [20]. Finally, yet importantly, the European Data Space for Smart Cities and Communities [21], aiming at creating a cross-sectorial data space for smart communities.

Digital Sovereignty Policies

In the last years, the European Union has been increasing its efforts to increase its strategic autonomy and sovereignty, with specific reference to the digital ecosystem. From a high-level perspective, this follows different key directions, on the one side through actions to increase the bloc's competitiveness, as anticipated in the introduction to this chapter, and on the other side through tailored strategic, policy and funding initiatives supporting the development of a stronger, more cohesive and integrated European digital ecosystem. The concept of 'digital sovereignty' is embedded, more or less explicitly in several policies and strategies at EU level, including the AI Act [22], the AI Continent Action Plan [23], the Apply AI Strategy [24], the Chips Act [25], the Quantum Europe Strategy [26], the proposed Digital Networks Act [27], the Data Act [8] and the Data Union Strategy [28], covering a wide range of facets of the European digital ecosystem and economy. Finally, yet importantly, the Commission has recently introduced the Tech Sovereignty package [29] which includes the Strategic Roadmap for Digitalisation and AI in Energy [30] the Communication on European Tech Sovereignty [31], the Cloud and AI Development Act [32] and the Chips Act 2 [33].

The EU is engaged quite broadly in promoting mutual technological compatibility and legal recognition of electronic signature systems, including Japan and India [13]. This will enhance cooperation and mutual support in areas of Digital Public Infrastructure, a key area of development in all the countries studied, closely related to avoiding lock-in to hyperscalers

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

(particularly US and Chinese companies) for critical national infrastructure. Joint development of pooled digital sovereignty across the broad range of Continuum platforms and protocols can use this approach as a guideline.

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

CONCLUSIONS

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

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

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

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

Suitable non-profit governance arrangements for FLOSS and Open Hardware need support in research and innovation from Horizon Europe or direct Commission support. A majority of the current FLOSS projects underpinning development are currently based in the US, subject to US jurisdiction and vulnerable to capture by US commercial and government interests. Forking

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

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

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

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

REFERENCES

References

[1] European Commission, “Joint Communication to the Parliament and the Council: International Digital Strategy for the EU,” 2025.

[2] European Commission, “Digital Decade Policy Programme 2030,” 2022.

[3] European Commission, “Commission Communication: A Competitiveness Compass for the EU,” 2025.

[4] European Union, “Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act),” 2024.

[5] European Union, “Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act),” 2019.

[6] European Union, “Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act),” 2022.

[7] European Union, “Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Martkets Act),” 2022.

[8] European Union, “Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act),” 2023.

[9] European Union, “Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act),” 2022.

[10] European Union, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation),” 2016.

[11] R. Adler-Nissen and K. A. Eggeling, “The Discursive Struggle for Digital Sovereignty: Security, Economy, Rights and the Cloud Project Gaia-X,” *JCMS: Journal of Common Market Studies,* vol. 62, no. 4, pp. 993-1011, 2024.

[12] European Commission, “Cloud Sovereignty Framework (version 1.2.1, October 2025),” 2025.

Co-funded by the European Union

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

[13] European Commission, “Annex 1 to the Joint Communication: International Digital Strategy for the EU,” 2025.

[14] European Data Protection Supervisor, “European Data Protection Supervisor Annual Report,” 2024.

[15] European Commission, “Commission Communication A European strategy for data,” 2020.

[16] European Commission, “Commission Staff Working Document on Common European Data Spaces SWD(2024) 21 final,” 2024.

[17] European Commission, “Commission Communication An EU Agenda for Cities: Driving Growth and Prosperity COM(2025) 739 final,” 2025.

[18] European Commission: Directorate-General for Research and Innovation, “EU mission, climate-neutral and smart cities,” Publications Office of the European Union, Luxembourg, 2025.

[19] European Commission, “Citiverse,” 14 05 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/factpages/citiverse.

[20] European Commission, “Interoperable Europe,” 17 June 2025. [Online]. Available: interoperable-europe.ec.europa.eu/collection/ldttoolbox.

[21] European Data Space for Smart Communities, “European Data Space for Smart Communities,” 2021. [Online]. [Accessed 29 May 2026].

[22] European Union, “Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Artificial Intelligence Act,” Official Journal of the European Union, Brussels, 2024.

[23] European Commission, “Commission Communication AI Continent Action Plan COM(2025) 165 final,” 2025.

[24] European Commission, “Commission Communication Apply AI Strategy,” 2025.

[25] European Union, “Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe’s semiconductor ecosystem (Chips Act),” 2023.

[26] European Commission, “Commission Communication Quantum Europe Strategy: Quantum Europe in a Changing World COM(2025) 363 final,” 2025.

[27] European Commission, “Proposal for a Regulation on digital networks (Digital Networks Act) COM(2026) 16 final,” 2026.

Co-funded by the European Union

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

[28] European Commission, “Commission Communication Data Union Strategy: Unlocking data for AI COM(2025) 835 final”.

[29] European Commission, “Commission proposes tech sovereignty package to strengthen Europe's digital autonomy and resilience,” 3 June 2026. [Online]. Available: Commission proposes tech sovereignty package to strengthen Europe's digital autonomy and resilience.

[30] European Commission, “Commission Communication Strategic Roadmap for Digitalisation and AI in the Energy Sector COM(2026) 501 final,” 2026.

[31] European Commission, “Commission Communication on European Tech Sovereignty, accompanied by an EU Open Source Strategy COM(2026) 503 final,” 2026.

[32] European Commission, “Proposal for a Regulation establishing a framework of measures for strengthening Europe’s cloud and AI ecosystem (Cloud and AI Development Act) COM(2026) 502 final,” 2026.

[33] European Commission, “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a framework of measures for strengthening the Union’s semiconductor ecosystem, repealing Regulation (EU) 2023/1781 (Chips Act 2.0) COM(2026) 504 final,” 2026.

GLOSSARY

FLOSS: Free, Libre and Open Source Software

IIoT: Industrial Internet of Things

PII: Personally Identifiable Information

Co-funded by the European Union

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