EUROPEAN
COMMISSION

Brussels, 3.6.2026
COM(2026) 503 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

on European Tech Sovereignty, accompanied by an EU Open Source Strategy

1. Introduction: the European vision of technological sovereignty

The European Union stands at **a defining moment to assert its *technological sovereignty*** and reclaim its place in the global race for geoeconomic power. The Draghi Report highlighted the epochal challenge ahead: despite years of regulatory leadership and sustained investments, the EU remains structurally reliant on non-EU providers for over 80% of its digital products, services, infrastructure and intellectual property[1]. As geopolitical fragmentation deepens and supply chains are increasingly weaponised, excessive technological dependencies in critical sectors are becoming strategic liabilities. This is even more the case as higher and rising energy costs in Europe are impairing its competitiveness, particularly in energy-intensive technologies like cloud or AI. The Union's technological sovereignty and economic security will depend on staying ahead in critical technologies, lowering our exposure in terms of existing strategic dependencies, and avoiding new dependencies that third countries can weaponise. In a world of rapid technological acceleration and intensifying strategic rivalry, the EU thus faces the risk of a structural erosion of its industrial and technological base, unless it acts decisively to close its innovation gap. This requires a rapid **shift of the EU's posture from a *reactive* focus on resilience and risk mitigation to an *assertive* and *proactive* approach grounded in technological sovereignty**.

Technological sovereignty denotes Europe's ability to develop, control and scale the critical technologies, infrastructure, services and data, including digital ecosystems, that underpin its economy, security and society, while derisking and diversifying supply chains and technological exposure to reduce strategic dependencies and resist foreign interference[2]. This requires:

i) Boosting indigenous innovation, homegrown industrial capacity and autonomy at each step of the supply chain of digital technologies, progressing towards a full European technology stack[3], while increasing the choice for end users in the digital single market;
ii) securing the supply of digital technologies underpinning Europe's competitiveness including by diversifying supply chains and reducing dependencies particularly on a single or a limited number of non-EU suppliers, including via trusted trade and investment partnerships;
iii) gain and maintain control over data infrastructures and critical data, while developing the capacity to effectively leverage them; and
iv) lead the standard setting for key strategic technologies, also in cooperation with partner countries.

Technological sovereignty is thus grounded in **openness, partnership and fair competition. It does *not* mean isolation, protectionism, or tech decoupling**. On the contrary, a technologically sovereign EU will continue to contribute to and benefit from integration in the global economy but will be better equipped to manage both the risks and the opportunities stemming from global technological interdependence. Strengthening Europe's technological base and independence in key digital supply chains creates strategic counterweights to boost Europe's capabilities and capacity to remain open to the world, without compromising its

[1] The Draghi report on EU competitiveness and Communication from the Commission 'State of Digital Decade 2025: Keep building the EU's sovereignty and digital future'. For Cloud, see also European Cloud Providers' Local Market Share Now Holds Steady at 15% | Synergy Research Group.
[2] JRC Publications Repository - Open but Not Powerless: Towards a Common Understanding of EU Digital Sovereignty.
[3] A technology stack is a set of technologies, software and tools that are used in the development and deployment of a single site, app, or other digital product (Resource: IATA).

interests and values. By strengthening partnerships, the EU will diversify supply chains, expand access to talent, infrastructure and innovation, and reduce vulnerabilities. A technologically sovereign EU will remain reliable and predictable partner, committed to deepening trusted relations and forging new, mutually beneficial technology partnerships with countries that share our vision of a secure, trustworthy, sustainable and human-centric future, while also promoting EU technology solutions abroad[4].

The *technological sovereignty package* ('the package') presented by this Communication marks the next step towards **achieving technological sovereignty** while remaining open to the world. It builds on the following EU initiatives that together form the policy and regulatory foundations of a coherent framework for asserting technological sovereignty[5]:

- the **Competitiveness Compass**[6] identifies closing the innovation gap, decarbonising the economy and reducing strategic dependencies as transformational imperatives for EU competitiveness;
- the **Digital Decade policy programme**[7] offers a strategic compass and monitoring mechanism for advancing reforms and investments in Europe's digital transformation[8];
- the **Communication on strengthening the EU's economic security**[9] sets out an integrated, whole-of-government framework and toolbox to proactively advance the EU's economic security interests, reduce the EU's exposure to risks, and prevent its de-risking objectives from being undermined, including through a more assertive and proactive use of such toolbox;
- the **Affordable Energy Action Plan**[10] offers a set of concrete short-term and structural measures to provide competitiveness, affordability, security and sustainability for all consumers including businesses;
- the Joint Communication on an **international digital strategy for the European Union**[11] seeks to boost EU tech competitiveness and innovation capacity while working with partners and allies to support their own digital transition; and
- the **AI Continent action plan**[12] and related **ApplyAI strategy**[13] put Europe on the path to becoming a true AI continent, by coordinating investments in research, infrastructure and talent, as well as in standards, and governance to position the EU as a global leader in trustworthy, innovative AI.

On this basis, the package sets out a forward-looking approach to achieving technological sovereignty through the following interlinked initiatives:

- a **Chips Act 2.0,** building on the first **European Chips Act**[14], to strengthen Europe's semiconductor ecosystem and supply chain resilience including measures to boost domestic demand for chips;

[4] The EU Tech Business Offer | Shaping Europe's digital future.
[5] Initiatives covering critical technologies for space and defence sectors – which have their own security of supply frameworks applying to both defence and non-defence crisis-relevant products – are outside the scope of the current package.
[6] COM(2025) 30 final.
[7] Digital Decade Policy Programme 2030, established by Decision (EU) 2022/2481.
[8] Conclusions on European Competitiveness in the Digital Decade - Council Conclusions (5 December 2025).
[9] JOIN(2025)977 final.
[10] COM/2025/79.
[11] JOIN(2025) 140 final.
[12] COM(2025) 165 final.
[13] COM(2025) 723 final.
[14] COM(2022) 45 final.

- a **Cloud and AI Development Act ('CADA')** to unlock the potential of the EU cloud and AI industry, ensuring these technologies are developed and used in the EU, while addressing the risks associated with Europe's reliance on non-EU countries;
- a **strategy for EU open digital ecosystems (the 'open source strategy')**, included in this Communication, to reinforce Europe's autonomy across the entire technology stack by leveraging open source software while maintaining an appropriate level of cybersecurity; and
- a **Strategic Roadmap for Digitalisation and AI in the energy sector** to support the delivery of secure, clean and competitive energy for all consumers, including a **Delegated Regulation** for the rating of data centres that underpins the sustainability of European data centres and mitigates 'greenwashing' in this sector.

Mainstreaming the goal of technological sovereignty at the heart of the EU's growth strategy requires action by using the right levers (Section 2) and by **taking a true 'ecosystem approach'** (Section 3). This means leveraging the EU's research excellence – while increasing the commercialisation of innovative solutions –, strong industrial base and single market across the entire value chain to shape the technologies of tomorrow and ensure they serve its values, strengthen its economy and benefit EU citizens. This is a precondition for Europe's competitiveness, economic security, prosperity and strategic autonomy.

2. Levers of Europe's technological sovereignty

The EU's vision for technological sovereignty must be grounded in a **clear assessment of its critical technological dependencies**, notably those affecting its economic security, and their geoeconomic implications. Europe remains excessively reliant on non-EU suppliers for raw materials and renewable energy technologies, as well as for the supply of key components of advanced digital infrastructure including semiconductors, cloud computing and essential AI hardware and solutions – an example being specialised software, electronic components and manufacturing inputs imported from the US and East Asia. However, what was once efficiency-driven global interdependence and trade-fuelled growth is turning into a landscape where asymmetric dependencies create geopolitical vulnerabilities. This is a risk that Europe needs to urgently address. In fact, the past few years have seen a stark increase in the weaponisation of dependencies and in the use of unjustified or wide-ranging export controls, limitations to foreign direct investment in third countries, and outbound investments. Sanctions and other unjustified restrictive measures are routinely deployed, including directly or indirectly against the EU and the Member States, with serious consequences on our competitiveness, growth and stability.

In the current landscape, high market concentration and vendor lock-in by a few non-EU players across the technology stack may reduce competition, slow down innovation and leave public administrations, businesses and citizens vulnerable to economic and security risks. The recent semiconductor shortages are a stark demonstration of the extent to which supply disruptions can impact Europeans' lives, from cars manufacturing, healthcare equipment and energy infrastructure, to consumer goods across the EU.

Despite sustained efforts under the European Chips Act[15], the EU produces only **around 10% of global semiconductors.** It is excessively dependent on the US and East Asia for both mature

[15] The European Chips Act resulted in around EUR 80 billion of announced public and private investment commitments into Europe's semiconductor ecosystem, of which around EUR 52 billion of public and private investment is being implemented, alongside EUR 3.7 billion invested in pilot lines to bridge the gap between the EU's advanced R&I capabilities and their industrial exploitation.

and advanced nodes, including AI chips which are becoming increasingly important for core European industrial ecosystems[16]. As **for cloud computing infrastructure and services,** failing to capture the gains of the first internet-led digital revolution resulted into slower digital adoption across the EU and **heavy reliance on foreign providers**[17]. In addition, the EU's limited data centre capacity poses a significant threat to its ability to benefit from the digital transformation and adopt AI-driven solutions, notably those requiring low-latency compute capacity, and deters investments in the region. Beyond market dynamics, this dependency exposes the EU to actual risks relating to foreign jurisdictional data reach and surveillance, creating material risks to public order.

The package addresses the challenges above by acting on a number of levers to achieve two mutually reinforcing goals: (i) securing EU supply chains by taking an open strategic autonomy approach; and (ii) reinforcing the 'European way' to technological sovereignty.

(i) Securing EU supply chains by taking an open strategic autonomy approach

Three levers will contribute to reaching this goal.

A first lever is to build a **'European technology stack'** to boost the EU's capacity throughout the value chain. To tackle the investment gaps, scaling barriers and skills shortages, Europe must improve its ability to develop, deploy and operate its own critical technologies – from advanced semiconductor design and manufacturing to cloud infrastructure, AI and digital technologies across all sectors of the economy and society, including among others mobility, aerospace, space and defence[18]. Without sufficient own capacity, paired with cooperation with trusted partners, Europe cannot safeguard its economic security, close its competitiveness gap, reduce dependencies, or shape global technological standards[19]. This includes promoting the EU tech business offer abroad, including via the **Global Gateway** and the **Pact for the Mediterranean**, to scale-up digital investments and partnerships which contribute the most to EU security and competitiveness and meet our partner countries' interests.

The actions set out under the **open source strategy** contribute to this objective of diversification – aiming to promote open European alternatives across the technology stack. Likewise, the **CADA** aims to support the development and uptake of highly innovative and sovereign cloud and AI technologies, and **the Chips Act 2.0** aims to reinforce Europe's semiconductor ecosystem and supply chain resilience. This approach builds on the previous experience of **the EuroHPC Joint Undertaking**[20], supporting a world-class data and computing infrastructure financed by the EU and Member States, governed by EU rules and in line with EU priorities. Under the **AI Factories**[21] **initiative,** EuroHPC has now evolved into

[16] State of the Digital Decade Report 2025 and State of the Digital Decade Report 2026 (to be published in June 2026).
[17] Although the EU cloud services market is growing, the market share of EU providers fell from 29% in 2017 to 15% in 2022 and has remained unchanged since – leaving over 70% of the market in the hands of three US hyperscalers.
[18] The EU Observatory of Critical Technologies (OCT) monitors and analyses critical technologies, related developments and supply chains of space and defence.
[19] Important Projects of Common European Interest (IPCEI), which are meant to create an EU ecosystem of companies, can contribute to this goal. So far one IPCEI on Cloud Information Services is being implemented since 2024, and others IPCEIs are being designed, including on Artificial intelligence (IPCEI-AI) and on a Compute Infrastructure Continuum. In particular, the IPCEI-AI will contribute to developing next generation technologies and necessary capabilities and skills for highly competitive AI solutions. The IPCEI on a Compute Infrastructure Continuum may establish a cross border, decentralised and federated compute infrastructure in the Union, and may be interconnected with the AI Gigafactories.
[20] The European High Performance Computing Joint Undertaking (EuroHPC JU).
[21] AI Factories | Shaping Europe's digital future.

an AI-optimised infrastructure, with **19 AI Factories**[22] and 13 AI Factory Antennas gradually becoming operational across Europe and enlargement countries.

Sovereignty is also at the core of the value proposition of AI Gigafactories (AIGFs)[23]**.** An official call for tenders is about to be launched to provide EU developers of advanced AI solutions with access to AI compute time and services for public and private stakeholders. AIGFs will provide the industrial-scale compute needed for the next generation of AI models and boost Europe's scientific capabilities and industrial competitiveness. Industry, academia and public administrations must be certain that strategic data and proprietary models remain under exclusive EU oversight to build the trust needed to migrate their most sensitive workloads. AIGFs ensure autonomous control over core physical and digital infrastructure and must be resilient against external dependencies and immune to foreign interference. By ensuring that the entire data lifecycle and all management services are governed by European standards and subject to EU jurisdiction, AIGFs will evolve from simple AI compute facilities into trusted environments for high-value innovation built on European values and under European law.

A second lever is **building trust in Europe's digital ecosystem** by fostering openness, (cyber)security and resilience. In a digital environment marked by growing market concentration and vendor lock-in, especially by non-EU providers, it is essential to safeguard cybersecurity across the technology stack. Equally, Europe's digital ecosystem must be interoperable, portable and based on the widespread adoption of open standards – to ensure that public and private users can choose, switch and scale technological solutions without prohibitive costs. Among other things, the **CADA** will promote open source, secure and sovereign solutions. It complements the **Data Act**[24]**,** improving interoperability and portability when switching cloud providers.

The **open source strategy** promotes secure, transparent and auditable[25] open source ecosystems for critical systems and digital infrastructures. The **CADA** and the **open source strategy** build on the framework developed by the **proposed revision of the EU Cybersecurity Act**[26]**,** which creates a certification and risk-management framework that can effectively limit the role of high-risk vendors in critical digital infrastructures. In parallel, the **EU Digital Identity**[27] and the **EU Business Wallet**[28] aim to create sovereign and interoperable digital identity systems, building trust and enabling secure digital interactions across borders.

A third lever is to **effectively manage technological interdependence making full use of trade, investment and cooperation with(trusted) partners, including for supply chain diversification purposes.** In a changing geopolitical environment and increasing technological competition, the EU must be able to mitigate critical dependencies, diversify supply chains and reduce excessive reliance on single non-EU suppliers or countries for key digital technologies. At the same time, it must maintain effective regulatory and operational control of its critical infrastructure, sensitive data and essential public services. This need is especially acute where

[22] AI factories are publicly supported AI infrastructure centres that provide shared supercomputing resources and datasets, often offering free or subsidised compute access to universities, startups and SMEs to accelerate AI research and innovation.
[23] EU launches InvestAI initiative to mobilise EUR 200 billion of investment in artificial intelligence.
[24] Regulation - EU - 2023/2854 - EN - Data Act - EUR-Lex.
[25] Open source can contribute to cybersecurity because public availability of source code enables independent inspection, audit and vulnerability detection, while facilitating peer review, coordinated remediation and software supply-chain transparency.
[26] EUR-Lex - Ares(2025)2970891 - EN - EUR-Lex.
[27] European Digital Identity - European Commission.
[28] COM(2025) 838 final.

the EU is heavily reliant on non-EU suppliers of technologies such as AI chips, cloud services and the underlying technology stacks.

For instance, recent semiconductor shortages[29] demonstrate how supply disruptions can translate into tangible impacts on daily life, affecting industrial automotive production, healthcare equipment, energy infrastructure and consumer goods across the EU, making supply chain resilience no longer just a purely industrial concern. This is why one of the objectives of the **Chips Act 2.0** is to boost the security of supply for semiconductors by reducing strategic technological dependencies and diversifying its supply. Pursuing a similar objective from a complementary perspective, the **CADA** requires governments to conduct sovereignty risk assessments in order to improve resilience, protect public order and choose European sovereign alternatives where necessary.

(ii) Reinforcing the 'European way' to technological sovereignty

Two levers will contribute to reaching this goal.

A first lever to purse this goal is to step up **sustainable innovation and investment.** This means investing in digital technologies that support decarbonisation, while helping to lower the high energy prices. Technological innovation and independence are in fact closely intertwined with the clean transition. The rapid expansion of digital infrastructure, including data centres, is considerably increasing demand for energy across Europe. By fostering the deployment of energy-efficient cloud infrastructure, the **CADA** responds to these needs by ensuring that the planning and deployment of new data centre capacity is in line with sustainability goals and strategic planning, helping to prevent additional pressure on limited natural resources and environmentally stressed regions. Energy-efficient and sustainable chip production and operation are prioritised in the **Chips Act 2.0**, in line with the EU's climate and energy goals.

The **Strategic Roadmap for Digitalisation and AI in the Energy Sector** aims to ensure the sustainable integration of data centres in the energy system through structured dialogue and voluntary commitments that maximise the use of clean energy, system flexibility, energy efficiency, and waste heat recovery. Additionally, the Strategic Roadmap will support the rapid and large-scale deployment of EU digital and AI solutions in key areas for decarbonisation, e.g. the electrification of industry, transport and households, better system integration across adjacent sectors, electricity grid optimisation, energy efficiency in buildings and industry and demand-side flexibility. A **Delegated Regulation on the sustainability of data centres** will put in place an EU-wide scheme to rate the sustainability of data centres in Europe using electronic labels issued by a European database. This is designed to increase transparency on their environmental performance and support the deployment of more sustainable digital infrastructure EU-wide.

A second lever is to take a **human-centric approach that upholds EU values** such as safety, security, transparency, human oversight, respect for fundamental rights, inclusivity, equality, non-discrimination and accessibility, in line with the **European Declaration on Digital Rights and Principles**[30], and to **maintain a level-playing field in the Single Market** underpinning competition, empowerment and participation. These values are embedded in EU legislation governing digital policy, underpinned by evidence and adopted by the EU's democratically

[29] E.g. the Nexperia case, in which the Dutch government intervened in the Chinese-owned chipmaker Nexperia, triggering tensions that disrupted the semiconductor supply chains.
[30] European Declaration on Digital Rights and Principles | Shaping Europe's digital future.

elected institutions. For example, the **Digital Services Act (DSA)**[31] enacts an all-of-society-approach to holding platforms and their business models accountable. It has ended the era where online platforms could produce entirely unchecked societal impacts. Today, platforms must assess systemic risks before they launch new features. Users are empowered to assert their rights, for example by challenging content moderation decisions. Similarly, the **Digital Markets Act (DMA)**[32] has been key to challenge structural imbalances in digital markets and promote fair business practices, market contestability and innovation. Technological innovation is not just a driver of economic growth. It is also a **cornerstone of Europe's just societal transition and social market economy**, essential for implementing the **European Pillar of Social Rights**, given the prevalence of digital technologies in the workplace. Therefore, the EU must ensure that digital advancements contribute to the creation of quality jobs and strengthen democratic resilience, solidarity, and freedom of choice, for instance by offering trusted and harmonised public digital infrastructure. In this package, the **CADA** promotes action to develop a sovereign cloud and AI stack, with the aim of strengthening the EU's technological autonomy, while preserving freedom of choice and inclusion. The assessment framework proposed by the **open source strategy** will recognise open source solutions that are in line with EU values and comply with EU regulations.

2.1 Horizontal enablers

In addition to action on these related levers of technological sovereignty, the EU must act upon key horizontal enablers of technological sovereignty:

- an **agile regulatory and business environment**, including a technology and innovation lifecycle approach as well as simplification and reducing administrative burden;
- adequate **digital skills**; and
- sufficient **financial firepower** for investments underpinning Europe's technological sovereignty.

The Commission is pursuing a tailored **technology and innovation lifecycle implementation logic**[33] and at the same time **simplifying** Europe's digital rules so that businesses can **spend less time on paperwork and more time on innovation in the digital single market**. The EU's digital single market rulebook is now composed only of a few horizontal acts covering AI, platforms, telecom, cloud, data, and personal data protection. In the future, the **Digital Networks Act**[34] will compile a joint rulebook directly applicable across the EU, replacing the European Electronic Communications Code[35], the BEREC Regulation[36], the Radio Spectrum policy programme[37] and core parts of the Open Internet Regulation[38]. On data policy, as part of the Digital Omnibus[39], the Commission has recently proposed to repeal the Data Governance Act[40], the Free Flow of Non-Personal Data Regulation[41], and the Open Data Directive[42] and to

[31] Regulation (EU) 2022/2065 – Digital Services Act.
[32] Regulation - 2022/1925 - EN - EUR-Lex.
[33] This refers to a coordinated and iterative development process enabling continuous iteration between discovery, development, testing and deployment, that accelerates the transition from research to innovation to the market.
[34] EUR-Lex - Ares(2025)4545535 - EN - EUR-Lex.
[35] Directive - 2018/1972 - EN - eecc - EUR-Lex.
[36] Regulation - 2018/1971 - EN - EUR-Lex.
[37] Decision - 2012/243 - EN - EUR-Lex.
[38] Regulation - 2015/2120 - EN - EUR-Lex.
[39] EUR-Lex - 52025PC0837 - EN - EUR-Lex.
[40] Regulation - EU - 2023/2854 - EN - Data Act - EUR-Lex.
[41] Regulation - 2018/1807 - EN - EUR-Lex.
[42] Directive - 2019/1024 - EN - psi directive - EUR-Lex.

consolidate key provisions into the **Data Act**[43]**.** In addition, targeted amendments proposed to the GDPR bring more legal certainty on lawful personal data used for training AI in Europe, bringing legal certainty to AI application. The **Digital Omnibus on AI** proposal[44] brings in a series of targeted changes to ensure the effective application of the rules in the **AI Act**[45]. The **Industrial Accelerator Act** proposal[46] accelerates permits and investment approvals for strategic industrial projects. The **European Business Wallet** proposal[47] simplifies business operations, regulatory compliance and cross-border interactions for companies as well as potentially the application of EU rules in other domains. Finally, the **DSA** and **DMA** set out complementary rules for very large online platforms and search engines, with a coherent enforcement structure at EU level, giving clarity and predictability to providers and users alike.

A skilled workforce is crucial to the competitiveness and resilience of the EU's digital ecosystem and to ensure that innovation can benefit everyone. Equipping individuals and businesses with the digital skills needed in the EU's digital economy is a central objective in the **Union of Skills** and its **STEM Education Strategic Plan**[48]. To this end, the package aims to boost the development of specialised advanced digital skills in semiconductors, cloud and open source, building on the priorities set out in the **Digital Decade policy programme**[49]. These include strengthening advanced education and training in emerging technologies and enhancing the attractiveness and mobility of students and workers, including from outside the EU, in STEM and ICT fields – in addition to an increased focus on foundational AI literacy. The **Strategic Roadmap for Digitalisation and AI in energy** includes funding measures to strengthen in-house digital and AI skills of energy companies.

Lastly, **to fund the sizeable investments needed for its technological sovereignty, Europe must achieve sustained financial investment capability**. The EU shall be able to mobilise large-scale strategic investment to innovate at scale, build critical infrastructure, and support the growth of homegrown high-potential and strategic technology businesses. This is especially the case in three technologies that will be essential for Europe's competitiveness and technological sovereignty – advanced digital technologies and infrastructure (e.g. AI, including AI Gigafactories and AI scale-ups, quantum technologies, semiconductors, cloud, 6G, and robotics); biotechnology (including biomanufacturing, drug discovery and synthetic production of construction materials); and clean energy technologies (especially batteries, motors, and power electronics, as well as small modular reactors). Advancements in each of these are mutually reinforcing: more computing power and clean energy improve AI capabilities; and more advanced biotechnology and a more powerful electric stack translate that progress into scientific and industrial gains. Finally, civilian technological breakthroughs in all these areas flow directly into the security domain. As regards the initiatives in the package, the investment needs for boosting the EU's semiconductor ecosystem are estimated at an additional **EUR 120 billion**. Expanding data centre capacity will require around **EUR 200 billion**, mostly from the private sector, by 2036[50], plus another **EUR 100 billion** for the full realisation of the Cloud and AI leadership initiatives, as well as the deployment of AI Factories and Gigafactories. Finally, for all measures under the open source strategy, an estimated **EUR 2**

[43] Regulation - EU - 2023/2854 - EN - Data Act - EUR-Lex.
[44] EUR-Lex - 52025PC0836 - EN - EUR-Lex
[45] Regulation - EU - 2024/1689 - EN - EUR-Lex.
[46] Carriages preview | Legislative Train Schedule.
[47] EUR-Lex - 52025PC0838 - EN - EUR-Lex.
[48] Union of skills - European Commission
[49] Decision - 2022/2481 - EN - EUR-Lex.
[50] CADA impact assessment.

billion will need to be mobilised by the public and private sectors over the next seven years. For energy, the annual investment gap is estimated at **EUR 400 billion**[51].

The above requires **leveraging public funding** more effectively and reducing fragmentation across financial instruments and national markets. The proposal for the EU's **2028-2034 multiannual financial framework**[52] has been designed with three objectives in mind: to have a more ambitious EU budget which is simpler, more impactful, flexible and more strategic to address current structural weaknesses and rigidities. Within this framework, the **European Competitiveness Fund (ECF)**, incuding in particular its **Digital Leadership Window**, are key to channel and leverage investments to pursue the goal of technological sovereignty, covering the full investment journey from collaborative research to innovation, industrial and infrastructure deployment, support for innovation ecosystems and their scaling up and resilience, and support to build advanced digital skills. The ECF operates as a dedicated investment capacity and aims to strengthen European competitiveness in critical technologies and strategic sectors. It will also act as a powerful enabler by using budgetary guarantees and financial instruments to crowd in private, institutional and national investments across the entire digital value chain, including targeted measures for startups, scaleups and SMEs. In addition to the ECF's direct investment role, a tight connection is ensured with the Horizon Europe programme (FP10) and complementary funding instruments, notably the **national and regional partnership plans (NRPPs)**. Under these plans, action on technological sovereignty can be reinforced at Member State level[53], aligning with common competitiveness priorities and enabling coordinated support to key areas and projects of strategic European interest. **European Digital Infrastructure Consortia** (EDICs) will also remain an important instrument to pull Member State resources to implement multi-country projects in sectors where the EU needs greater technological sovereignty, such as education and skills.

At the same time, public funding alone cannot close Europe's investment gap, which calls for further deepening and integrating the EU's capital markets and effectively designing public funding instruments in order to **crowd in massive volumes of private capital.** The reform of the EU's capital markets under the **Savings and Investment Union** will progressively improve how the EU's financial system channels savings to productive investments and provides EU businesses with a range of efficient financing opportunities. At the same time, Europe must urgently tackle its structural shortage of private risk capital,and in particular equity, for high-growth and deep-tech companies as well as large infrastructural investments. The **InvestAI initiative**[54], which aims to mobilise EUR 200 billion in AI, illustrates the scale of investment needed just in this specific area to fulfil our technological ambitions.

3. The EU response: an 'ecosystem approach' to tech sovereignty

Achieving EU technological sovereignty requires **developing a new ecosystem approach** across the entire value chain and combining multiple instruments:

i) demand-side measures;
ii) supply-side measures and support for strategic projects; and
iii) measures to improve enabling conditions across all sectors ('horizontal enablers').

[51] Clean energy investment – Energy – European Commission.
[52] EU budget 2028-2034.
[53] This includes cities-anchored innovation, reflecting local needs and enabling cities to drive EU technological advancements.
[54] EU launches InvestAI initiative to mobilise EUR 200 billion of investment in artificial intelligence | Shaping Europe's digital future.

For the first time, the Commission is putting forward a multi-pronged, comprehensive strategy to achieve tech sovereignty, with initiatives that are interconnected and mutually reinforcing across each stage of the value chain (from chips, to infrastructure, to software, cloud and AI), and in synergy with past and ongoing initiatives such as AI Factories and AI Gigafactories (AIGF). This 'ecosystem' approach responds to a strategic need: measures to reduce excessive supply dependencies and boost domestic capacity in Europe must go hand-in-hand with measures to create demand in downstream sectors, in line with the goals to boost open strategic autonomy and reinforcing the 'European way' to technological sovereignty. In turn, the approach is flanked by measures to improve the enabling conditions to attract foreign high-potential and strategic technology businesses to Europe and improve competitiveness. The enabling conditions include innovation, favourable cost factors, skills and sufficient financial firepower to invest in strategic tech projects EU-wide. No other strategy is likely to deliver the same results.

The above-mentioned ecosystem approach is clearly reflected in the various initiatives that make up this package, including the **Chips Act 2.0**, the **CADA** and the **open source strategy** presented in Section 4. The sections below show how the different components of the package come together and are consistent with other past and ongoing initiatives such as AIGFs.

3.1 Demand-side measures

While the **Chips Act** mostly focused on supply-side measures, the **Chips Act 2.0** will also cover the demand side. Demand for European semiconductors could double by 2040, driven primarily by consumer electronics, the automotive sector, energy and data centres. Of these sectors, data centres are projected to experience the most significant growth in consumption demand. Demand is also forecast to grow across all node ranges, with the steepest increase expected for sub-16 nm nodes, fuelled by AI and advanced logic technologies. To capitalise on this trend, Chips Act 2.0 aims to stimulate demand for high-performance AI chips by leveraging AI infrastructure initiatives, including AI Factories and Gigafactories, as well as cloud-related measures under the CADA. This is in line with the approach to cover the whole stack – from hardware to software – to reinforce Europe's technological sovereignty.

Each AIGF will in fact operate at industrial scale, with at least the equivalent compute performance of 75 000 advanced AI compute accelerators. Through **demand accelerators**, the Chips Act 2.0 will also aim to boost the use of EU-designed and EU-made chips for example, by allowing technology initiatives and strategic projects to showcase the semiconductor-related products to the potential industry users via a demand forum. It will also support collaboration on custom chip design with industry involved at an early stage of development. To stimulate demand and support EU-based startups and scaleups, the Chips Act 2.0 will encourage **public innovation procurement** as a strategic tool to create a clear and structured pathway to purchasing semiconductor technologies developed in the EU. Additionally, to enhance supply chain resilience by decreasing overreliance on certain suppliers, contracting authorities and contracting entities may require more transparency in the sourcing of semiconductors incorporated into critical infrastructure by considering security of semiconductor supply elements in public procurement procedures[55].

[55] Both the Chips Act 2.0 and the CADA are coherent with the Better Regulation Communication and its actions related to public procurement. Both Acts contain a sectoral instrument related to the procurement respectively of critical technologies containing semiconductors and of cloud computing services. Through this, both Acts aim to enhance supply chain resilience and decrease overreliance on certain providers. The two Acts do not regulate how contracting authorities and contracting entities procure but: (i) the Chips Act 2.0 allows for contracting authorities and entities to require more transparency related to

A **cybersecurity risk assessment** will identify and evaluate any technical vulnerabilities and non-technical factors to prepare for the proposed revision of the Cybersecurity Act. Lastly, the Chips Act 2.0 will set **grand challenges**[56] to help generate early demand and facilitate faster market entry for semiconductor technologies developed in the EU.

Consistently with this approach, measures under CADA to accelerate the deployment of data centre infrastructure in the EU are expected to generate a demand-side effect. By supporting the development of such infrastructure, these measures can strengthen the conditions for the uptake of European technologies. Moreover, CADA's objective of achieving security and autonomy across the cloud and AI stack is closely linked to the development of processors and accelerators designed and, where appropriate, manufactured in the EU. In this broader sovereignty context, CADA also establishes a **Union cloud and AI sovereignty framework** for cloud computing services, comprising four distinct sovereignty assurance levels. These levels are defined by criteria related to control over the service and software supply chain, processing of AI inference data, location of the infrastructure, assets and personnel, and level of cybersecurity. Member States and Union entities will need to conduct a **sovereignty risk assessment** to determine which of level of assurance is necessary for each use case. The Commission will provide guidance to facilitate this process and ensure a consistent approach across the Union. By introducing these sovereignty assurance levels, the CADA aims to provide a transparent and reliable way to assess the sovereignty of cloud computing services, especially for the public sector. This is expected to facilitate a more informed uptake of sovereign cloud computing services. The Act will also promote the use of EU added value in the public procurement of cloud and AI.

The energy sector presents a pivotal opportunity for the EU to assert global leadership in industrial innovation. Being a global frontrunner in energy-related industrial applications[57], the EU must capitalise on its strengths to lead the next generation of digital energy technologies. The **Strategic Roadmap for Digitalisation and AI in energy** underscores this ambition, supporting the development of sovereign digital and AI tools, trained on European data and developed by EU firms. Given the energy sector's strategic importance, ensuring that critical digital technologies are developed and governed in the EU is not just a competitive imperative but a cornerstone of the EU's technological sovereignty.

Lastly, the **open source strategy** focuses on reinforcing open source communities in Europe. It promotes the adoption of open source solutions by the public and private sectors with the goal of reinforcing the EU's technological sovereignty. It prioritises solutions that are already mature and that can take root as genuine alternatives or as new markets. In particular, the roll-out of the European Business Wallet and the EU Digital Identity Wallet, which are based on open source solutions, offers significant potential to broaden demand and stimulate ecosystems around their core technologies.

3.2 Supply-side measures and strategic tech projects

On the **supply side,** the **Chips Act 2.0** will increase Europe's capacity in mainstream and advanced semiconductors, also building on the measures aimed at boosting the supply side of the value chain already introduced by the Chips Act. The Act proposes strategic projects,

what is intended to be procured; and (ii) the CADA requires them to use non-price award criteria to evaluate the tenderer's contribution to the development of a European cloud and AI ecosystem under specific circumstances.

[56] Grand challenges are defined as large-scale, cross-sectoral initiatives addressing major technological and industrial challenges of strategic relevance for the Union.

[57] IEA - Energy and AI, World Energy Outlook Special Report, 2025.

including an EU-based open foundry for advanced semiconductor manufacturing to produce AI chips and other semiconductors with node size of 3 nanometres and below. It will be the first-ever EU semiconductor plant combining leading-edge node chip manufacturing with chiplet integration and 3D packaging. Pilot production could be envisaged by 2030-2033. The EU, Member States, and industry will be joining forces under the **Competitiveness Coordination Tool** to establish such a strategic project, while promoting demand, coordinated investment and reforms to maximise impact in a sovereign and innovation-rich semiconductor ecosystem. The Act will also clarify the scope of the Chips Act provisions on **first-of-a-kind facilities** to cover all key segments of the semiconductor value chain, including specialty materials, equipment, printed circuit boards, advanced packaging, assembly and facilities for manufacturing-centred chip design activities, which will make it easier to apply the provisions to strategic projects. The Commission will seek to further simplify and accelerate the State aid assessment of these projects, while preserving the level-playing field in the internal market. This reflects the Commission's commitment to reducing the administrative burden and to increasing speed, which is particularly critical in the fast-moving semiconductor sector to strengthen Europe's technological sovereignty.

The **Chips Act 2.0** also emphasises action to **accelerate the industrialisation of pilot lines**, transforming successful pilot manufacturing facilities into commercially viable manufacturing capabilities. It adds **photonics and photonic-integrated circuits** as an additional component in the Chips for Europe Initiative[58], as they are key enabling technologies for a wide range of strategic sectors, including telecommunications, data centres, AI, sensing, healthcare, automotive, aeronautics and quantum.

The **CADA** introduces a framework that simplifies and harmonises EU-wide data centre deployment. The objective is to triple capacity over the next 5-7 years, and to ensure that the EU has the necessary capacity to meet its needs by 2035. This will be achieved while ensuring high sustainability standards and balanced geographical deployment across Member States. The **CADA** also includes a mechanism to identify and support strategic projects. This will prioritise support for data centres with significant built-in innovation and sustainability, as well as those that contribute to the balanced distribution of computing capacity. The Act also sets out key cloud and AI challenges with the goal of developing a complete and integrated technology stack, including both the cloud and AI layers.

The **Strategic Roadmap for Digitalisation and AI in energy** seeks the sustainable integration of data centres in the energy system through structured dialogue and voluntary commitments that maximise the use of clean energy, energy system flexibility, energy efficiency, and waste heat recovery.

The **open source strategy** includes actions and strategic projects to turn mature open source building blocks into more widely used solutions across the technology stack, while supporting the development of new solutions in areas where strategic dependencies remain and where open source solutions can help to diversify the market, such as operating systems and AI algorithms. As illustrated by the beta launch of the **EU age verification app**, open source communities can help stress-test solutions, identify bugs and make them more robust.

[58] The Chips for Europe Initiatives (Pillar I) had previously five key components: pilot lines, the Design Platform, quantum chips, Competence Centres and the Chips Fund.

3.3 Horizontal enablers

Boosting investments

Given their large-scale and innovative nature of EU-wide interest, financing these projects calls for an 'ecosystem approach' going beyond the traditional funding model based on grants, in favour of a risk-capital one rewarding the whole investment journey. This includes boosting innovative investments across all critical sectors that are part of the EU's Economic Security Strategy. For instance, a competitive and secure energy supply is a precondition for technological sovereignty, and capital-intensive investments in clean energy require equity, including small modular reactors and storage systems to lower energy costs for digital infrastructure such as HPC or AI Gigafactories. The same applies to the capital-intensive investments in biotech necessary to fully benefit from the AI revolution. In all these cases, the timing of action is critical. In AI-related infrastructure, for instance, scale dynamics create tipping points: once a limited number of platforms reach sufficient scale and utilisation, cost advantages, data accumulation and ecosystem effects become self-reinforcing. Europe still has a window of opportunity to reach such tipping points in areas such as compute and cloud infrastructure, but this window is narrowing, as investment decisions, long-term contracts and location choices are being locked in rapidly. Delayed action would not only leave Europe's position unchanged but risks entrenching existing dependencies, making later rebalancing significantly more difficult and costly. As such, swift and large supply of equity for large-scale strategic projects will increasingly be a key determinant of Europe's technological sovereignty.

Europe suffers from a huge gap in terms of equity and high-risk financing. A first important answer to this issue is offered by the **Scaleup Europe Fund**. However, EU companies are more likely to suffer from insufficient equity financing than their US and international peers and depend predominantly on standard debt financing, which is unsuitable to fund innovative projects in early stages or large-scale investments. The share of global venture capital funds raised in the EU is only 5%, compared to 52% in the US and 40% in China. Moreover, China controls nearly 20% of global Sovereign Wealth Fund assets – i.e. USD 2.4 trillion, compared to USD 80 billion by the EU. Sovereign wealth funds and public pension investors also allocate little capital to Europe relative to the US (which attracted half of total global investment in 2025) and a few Asian markets. These weaknesses are acute in advanced technologies. High-growth deep-tech companies requiring patient risk capital, such as AI or quantum startups and scaleups, increasingly relocate outside Europe, being financed by non-EU investors as they reach critical scale-up phases, or are taken over. This is why the International Monetary Fund (IMF) has recently called for investments in digital innovation, energy and defence to be regarded as EU public goods to be paid for through joint financing[59]. Doing so, the EU would align with major international partners such as Canada, which has recently announced the intention to create a sovereign wealth fund for strategic investments.

There is indeed the need for an urgent reflection on the means to boost a European equity capacity at scale to finance Europe's tech sovereignty ambitions. The focus of this reflection would be the feasibility to set up an asset management mechanism to manage a portfolio of equity investments in advanced technologies and infrastructure in critical sectors

[59] See IMF – Press Briefing Transcript: European Department, Spring Meetings 2026.

as per the 2023 Economic Security Recommendation (such as AI, semiconductors, quantum, robotics, biotech, as well as clean energy technologies) plus potentially defence tech. The main advantage of this mechanism would be to create a much-needed **equity 'co-investment anchor' crowding in large amounts of private investments**, by working in synergy with or investing in financial instruments already existing at EU level, in particular to expand their equity stake or provide follow-on financing for key EU strategic projects on equal foot with private investors on a market conform basis. As existing instruments have specialised in improving access to risk financing for innovative companies or supporting early-stage industrial scale-up through comparatively small-scale interventions and small-ticket sizes, or deploying largely non-equity operations (loans, quasi-equity, venture debt) or 'fund-of-funds' model, such new mechanism would complement them, primarily for companies larger than scaleups and by investing in large-scale tickets particularly in tech infrastructure – acting not only as a de-risking partner but also as a market aggregator for technological sovereignty, maximising leverage and strategic impact in funding risky breakthroughs Europe needs to close its innovation gap.

An initial one-off injection of public capital in this mechanism supporting strategic projects might be needed to kick-start a virtuous cycle of reinvestment of returns from successful equity investments. The initial capital endowment of such mechanism could come from EU funding programmes or national contributions. However, some degree of leverage through loans could be considered. In particular, it might be possible to explore mechanisms by which national contingent liabilities to support such common investments might not have a direct impact on the participating Member States' public finances. Finally, such mechanism should encourage ample participation into its capital from private investors, including potentially retail investors. In the next MFF, the instrument of election to finance such mechanism could be the ECF, but other programmes such as the NRPPs could also contribute. Consequently, part of potential investment yields could be channelled as EU budget revenue. As regards the ECF InvestEU Instrument, such mechanism would have the potential to become an important implementing partner for strategic equity investments for large tickets in advanced technologies and infrastructure.

The Commission intends to consult Member States, the EIB Group, as well as other key stakeholders on how to set up such new mechanism. Following the consultation phase, the Commission will present its findings, which might be accompanied by a legal proposal. By mobilising hundreds of billions in private investments in advanced technologies and infrastructure in critical sectors for our economic security, a new strategic tech equity capacity for Europe could be an important success factor to achieve the EU's technological sovereignty ambitions.

An agile regulatory and business environment

The second key enabling condition is an agile regulatory and business environment, including a technology and innovation lifecycle approach**.** On this front, the **Chips Act 2.0** contains provisions ensuring that semiconductor technology facilities and strategic projects qualify for accelerated environmental approval under the EU's fast-track permitting rules. Secondly, building on the first simulation exercise on semiconductors supply chain disruptions conducted with Member States in 2025, the Commission will develop an **EU Blueprint for semiconductor crisis management** by Q2-2027. Similarly, the **CADA** aims to accelerate data centre deployment by harmonising investment conditions, focusing on sustainability and

innovation. In designated areas, operators would benefit from simplified procedures to access land and reliable energy infrastructure, as well as from funding opportunities across the EU.

Additionally, private investors must have good visibility over the investment potential across the EU for the newly unlocked investments to produce the most value added for the European tech ecosystem. To this end, the Commission will develop an EU-level promotion initiative giving **streamlined access to information on the investment needs and readiness**. Information regarding investment needs and readiness will be accessible to investors from the EU and non-EU countries alike. It will provide a matchmaking function enhancing the visibility of the Semiconductor Regions of Excellence introduced by the Chips Act 2.0, the Data Centre Acceleration Zones established by the CADA and highly innovative ecosystems assisting the implementation of the Apply AI sectoral flagship initiatives (for example the 'Autonomous Drive Ambition Cities').

Skills

The third enabling condition is **highly skilled human capital.** In order to achieve technological sovereignty, education systems must build competences cumulatively — from basic skills in compulsory schooling through higher and vocational education to lifelong learning. Foundational digital competences and AI literacy acquired in schools are the bedrock on which specialised expertise is later built.

Building the specialised ICT skills needed to achieve EU technological sovereignty requires effective coordination and governance across responsible public authorities, industry, academia and training providers, mindful of regional specificities. At the EU level, an example is offered by the **Digital Skills Academies**[60]. Priorities include upskilling and reskilling the existing workforce, supporting workers to transition out of declining sectors and stepping up advanced education and training in those emerging technologies. Equally critical is the need to boost the attractiveness of STEM fields and to foster student and worker mobility, including bringing in talent from outside the EU, to ensure Europe can compete and innovate at the frontier of the global digital economy. The **European Legal Gateway Office**, launched in early 2026, is a first pilot to attract the best ICT students, researchers and professionals from a non-EU country, by harnessing legal migration pathways.

[60] In particular, the existing Digital Skills Academy on cybersecurity and the upcoming ones on AI, quantum and semiconductors, to be launched on 30 June 2026.

4. A strategy for EU open digital ecosystems: leveraging open source to strengthen Europe's technological sovereignty ('open source strategy')

Open source[61] **crucially contributes to achieving the EU's technological sovereignty**, as it often underpins key areas, such as critical communication, commerce, healthcare, scientific research and government services. Europe, the birthplace of Linux, is home to a strong and vibrant community of over 3 million open source contributors[62], delivering digital solutions aligned with European principles and values[63]. The open source ecosystem forms part of a wider innovation ecosystem that helps to boost Europe's competitiveness by accelerating innovation, lowering technology costs, reducing dependence on foreign vendors, and enabling local companies, researchers and governments to build secure, customisable and globally competitive digital solutions with relevant safeguards for cybersecurity risks.

The EU currently spends EUR 264 billion a year mostly on US proprietary IT products and services[64]. This creates dependencies that affect Europe's ability to control key digital infrastructures, reduce lock-in risks and ensure security and compliance[65]. **Europe's strong open source capabilities offer a path to avoid this dependence**. However, the ecosystem faces several challenges: a lack of sustained funding after the early stage of a project, uncertainty regarding maintenance and security, accessing capital for scaling up, low brand recognition and barriers to public procurement. Global open source ecosystems are increasingly shaped by non-EU countries, notably by the US and, in an increasingly strategic manner, by China. Europe must therefore ramp up its presence to provide not only code and talent but also vision and leadership.

EU legislation and policy already provide support for open source[66]. Building on current policy, this **open source strategy** sets out four objectives to:

i) leverage open source for technological sovereignty;
ii) strengthen and promote a vibrant open source ecosystem;
iii) promote open and interoperable digital ecosystems for public administrations, including EU institutions; and
iv) reinforce digital standards and international outreach.

[61] For the purpose of this Communication, 'open source' refers to software released under licences that comply with the Open Source Initiative's Open Source Definition, which requires, among other criteria, availability of source code, permission to create derivative works and non-discrimination against persons, groups, or fields of endeavour. In terms of licensing, this is software distributed under OSI-approved licences (including, for example, widely used licences such as GPL, Apache-2.0, MIT, MPL-2.0, EPL-2.0, as well as the EU's own EUPL).

[62] Linux Foundation, What's the State of Open Source in Europe? And Why Does It Matter Now? and GitHub Innovation Graph data.

[63] Among the longstanding European success stories for open source and open science, CERN (the European Organization for Nuclear Research) has released the source code for the World Wide Web software and developed and scaled widely used open infrastructures such as ROOT.

[64] Cigref Study, Technological Dependence on American Software and Cloud Services, Asterès Research, 2025, p. 2.

[65] European Parliament, Policy Department for Transformation, Innovation and Health, European Software and Cyber Dependencies, PE 778.576, 2025.

[66] The Interoperable Europe Act defines 'open source licence' and backs collaborative development and reuse across the public sector via the Interoperable Europe framework and portal. The AI Act recognises free and open source models and sets proportionate transparency duties. The Cyber Resilience Act introduces the concept of open source software stewards and enables voluntary security-attestation programmes for FOSS components. The EUDI Regulation makes open source a legal default for the EUDI Wallet, by establishing that application software components must be open source, with narrowly justified exceptions. The proposed EU Business Wallet also mandates reuse of EUDI standards, trust framework components and open formats, creating structural advantages for open source implementations even where licensing remains market driven.

The strategy includes **supply-side measures** to enable EU communities and companies to develop, scale up, maintain and secure high-quality open source components. It also includes **demand-side measures** to accelerate private and public sector adoption, integration and deployment of secure open source solutions.

The strategy combines **public funding with market and demand-driven measures,** emphasising co-production with Member States, open source communities and the private sector. It builds on over 1 600 contributions to the Commission's call for evidence from a broad range of stakeholders. This strategy also highlights how the Commission, as a major public administration and policymaker, will use and develop open source and open technologies more broadly, contributing to a European open and sovereign digital ecosystem. It serves as a blueprint for other EU entities and public administrations EU-wide. The strategy aims to harness the power of open source to develop EU alternatives and strengthen Europe's strategic autonomy in critical areas of digital infrastructure where it currently faces dependencies. This is a direct response to the European Council's call to '*advance Europe's digital transformation, reinforce its sovereignty and strengthen its own open digital ecosystem*'.

The potential of open source

As their source code is publicly available, open source solutions can be freely used, modified, redistributed and audited. Open source is a strategic enabler for European competitiveness and technological sovereignty. By lowering the barriers to market entry, reducing strategic dependencies and promoting the reuse of digital building blocks, it can help reduce production costs, minimise user lock-in and foster collaborative innovation by enabling communities and companies to jointly develop, adapt and secure technologies[67]*. Open source can contribute to cybersecurity and helps identify and address cybersecurity vulnerabilities, to the extent that the transparency it enables wide public inspection. As the transparency allows to identify also the vulnerabilities of the source code, notably using AI , appropriate mitigation measures are needed. It is equally important for science, as access to source code supports reproducibility, enabling researchers to understand, validate, replicate and extend experiments.*

Open source projects operate under various models, for example: (i) independent, volunteer-driven and informal networks, sometimes hosted by foundations; (ii) projects managed by large companies (mostly non-European) that use open source for their core products but add proprietary layers for monetisation; and (iii) dedicated 'pure open source' companies that install, maintain and provide support services. The growing success of open source as a business model is evident in the rise of promising EU-based companies with industrial grade capabilities[68]*. This industry is growing at national level and has associations that promote these models at EU level*[69]*. Nonetheless, nearly half of all code commits in Europe come from small firms with fewer than 50 employees. These firms continue to face structural barriers to*

[67] This has been recently recognised also by the G7 Declaration 'Vision on AI openness opportunities and shared language' (May 2026).

[68] **Odoo** (Belgium) recently reached a valuation of EUR 5 billion with over 13 million users, and **Aiven** (Finland) raised USD 210 million to scale managed open source cloud services. In the field of artificial intelligence, **Mistral AI** (France) develops high-performance open-weight large language models as a sovereign alternative to closed-source systems. Many computer and service infrastructures use solutions by European companies, such as **SUSE Linux** (Germany) for operating systems, **Nextcloud** (Germany) for self-hosted collaboration and **Arduino** (Italy) for open source electronics. Furthermore, companies develop privacy-oriented tools such as **Matrix** for decentralised communication, **XWiki** and **CryptPad** for collaboration, and **OpenNebula** for cloud and edge computing.

[69] For example, APELL – The European Open source Software Business Association – represents national open source business associations in eight Member States (DE, DK, IT, FI, FR, NL, PT, SE).

scaling, branding and market integration, particularly in procurement and industrial deployment[70].

Over the years, the Commission has supported open source solutions and European open source communities across critical sectors, from internet technologies and cloud, to IoT and edge computing to AI, chips and cybersecurity (Annex II). While the EU has allocated EUR 800 million[71] *under the current multiannual financial framework, this funding lacks strategic focus on long-term sustainability of open source solutions and communities, which is key to maintaining sovereign digital solutions over the long term.*

4.1 Promoting and leveraging open source for EU technological sovereignty

To reduce dependencies on non-EU countries that can be weaponised, an initial assessment of dependencies has been carried out. Based on this assessment, targeted action is required to boost promising areas that already offer alternatives and to tackle the gaps identified in strategic domains.

The Commission will work together with the Member States and the private sector to:

i) support existing open source sovereign technology; and
ii) further develop open source solutions, in particular for critical technological areas.

Make available and facilitate the uptake of other existing EU sovereign technology solutions alternatives

To support the uptake of existing open source solutions as sovereign technology solutions, the Commission will carry out the following measures:

- Scale up the **Open Internet Stack**[72] to provide a shared catalogue, a one-stop shop for open source building blocks and sovereign solutions in Europe.
- **Increase awareness of the EU sovereign tech solutions available,** including by mobilising European, national and regional support networks (such as the Enterprise Europe Network). This includes providing tools for private and public organisations to **assess the sovereignty of their digital value chains**, building on existing initiatives[73] and the sovereignty framework introduced by the Cloud and AI Development Act.
- Promote the development and uptake of open source solutions across the **EU Digital Identity ecosystem,** anchored by the **Identity Wallet** (EUID) and the **European Business Wallet** (EBW). The Commission will:
    i) provide tools to support the interoperability, integration and reuse of open source stacks, including a Software Development Kit to support integration of the EUID into relying-party systems and an open source reference implementation protocol for legally valid communication channels for the EBW;

[70] Blind, K. et al. (2021). The impact of Open source Software and Hardware on technological independence, competitiveness and innovation in the EU economy, European Commission.
[71] Including investments in NGI, Open Internet Stack, SIMPL middleware, open source related AI (e.g. openEuroLLM) and Cybersecurity, RISC-V related investments.
[72] Under Horizon Europe work programme 2026-2027, the Commission has mobilised an investment of 41.3 million EUR through three calls: 'Open Internet Stack Sovereign Solutions', to deliver a large selection of open source solutions; a support action 'Open Internet Stack Support for Scale' and a call on the Web 4.0 architectural framework and Open Internet Stack applications for virtual worlds.
[73] Such as the index developed by the Digital Resilience Initiative, or the Software Sovereignty Scale.

ii) procure the development of open source solutions for the EBW, ensuring reuse of the European Digital Identity Framework standards and components;

iii) transfer the long-term stewardship of the open source reference implementations of the EUID and the EBW to the European Digital Public Infrastructure Foundation;

iv) provide support for implementing the fully open source age verification solution in cooperation with EUID open source communities.

- **Partner with Member States**, in particular with the European Digital Infrastructure Consortium (EDIC) on the Digital Commons[74]**,** and explore the possibility of launching an EDIC on digital education to **facilitate the development and/or adoption of secure open source alternatives**[75]. In the short term, the priority will be on domains where EU open source alternatives are established, such as cloud infrastructure and digital workplace applications, with the view to reach at least 30 million active users by 2030 for open source collaboration and productivity tools, instant messaging and secure email.
- **Strengthen the open source social media space[76]** by supporting open and decentralised social media solutions and platforms. The Commission currently runs a Mastodon instance, which hosts the Commission's presence and plans to extend the users basis to EU institutions.

In addition to the above, the Commission will promote the development of open source solutions in relevant calls for proposals across R&I programmes[77] as well as in calls for tender with the aim to help develop a full EU technology stack, paying attention to agile funding mechanism to facilitate participation of open source communities. Examples of key technology areas where open source building blocks and solutions could be further developed include:

- **semiconductors:** to develop, under the Chips Act 2.0, open source hardware IP such as the one based on RISC-V, targeted investment in open source electronic design automation tools;
- **operating systems:** computer operating systems, mobile operating systems, internet of things, robotics and drone operating systems;
- **future internet architecture**: software development & delivery infrastructure; open source building blocks for the Web 4.0 and architectural frameworks for virtual worlds;
- **cloud stack:** software stack supporting the European cloud-to-edge continuum, expanding across the compute, connectivity, data and AI service layers;
- **software development infrastructure (DevOps)** to accelerate software delivery, enhance security and improve code quality and federating tools for regulatory compliance, dependencies identification, and vulnerability management;
- **AI stack**: to focus on the development of open source AI models, taking into account the appropriate safeguards, including state-of-the-art model architectures, foundational models

[74] The Digital Commons European Digital Infrastructure Consortium (DC EDIC) was established on 29 October 2025 under Commission Decision (EU) 2022/2481 on multi-country projects as an EDIC dedicated to Digital Commons. It has legal personality and can own assets, sign contracts and receive EU and national funding.

[75] A possible EDIC on digital education would help forge closer Member State cooperation with a view to creating trusted and interoperable European digital education infrastructures, including a possible suite of open source software for schools and universities, laying the necessary conditions for the EU's EdTech companies to innovate and scale across borders.

[76] European citizens and businesses are heavy consumers of social media, but they rely almost entirely on foreign-owned, centralised, proprietary platforms.

[77] For instance, making research outputs, such as software, publicly available under an open-source license should count towards fulfilling requirements for actively disseminating project results.

and agentic frameworks and to prioritise the development of an open source software stack for AI Factories and AIGFs;

- **cybersecurity**: open source cyber threat intelligence frameworks, tooling for vulnerability coordination and disclosure, assurance and verification tools to strengthen the security of widely used open source components and support compliance with the Cyber Resilience Act.

Foster open source in industrial sectors

Leading European industrial players in key sectors such as the energy, automotive and aviation sectors have already taken the lead in setting up open source industrial platforms. In these platforms, competitors share non-sensitive information and develop common non-differentiated open source building blocks to increase efficiency, while continuing to compete on final products. Reducing dependencies, including through open source, in sectors critical for the economy and society is essential to the EU's economic security and prosperity.

The Commission will also leverage open source in critical sectors of the economy to reduce its dependencies on non-EU countries, especially in AI. For this, it will accelerate AI deployment and foster cross-sector collaboration. Specifically, the Commission will:

- **mainstream open source deployment in the Apply AI strategy calls,** focusing on strategic sectors such as automotive, energy, mobility, healthcare and pharmaceuticals, agri-food, robotics, manufacturing, geospatial and aerospace;
- support **industrial collaboration** platforms where competitors jointly develop open source building blocks[78] to create common software stacks and increase the overall efficiency of digital transformation, as demonstrated, among others, in the automotive[79], aviation, and railway sectors[80].

4.2. Strengthening and promoting a vibrant open source ecosystem

The EU is home to a strong ecosystem of developers, a nascent open source industry in key areas and new forms of cooperation between Member States (e.g. EDICs in areas such as the Digital Commons, IMPACT on public administration, or Europeum for Blockchain). It can now reinforce its competitive position across these models to make sure the whole ecosystem can thrive, and the EU economy benefit from the solutions created by EU developers.

Scaling up open source startups and open source business models

In line with the **EU startup and scaleup strategy**[81], the Commission will **leverage EU programmes and public procurement** to help transform open source initiatives into sustainable businesses. First, the Commission will put in place dedicated support actions[82] setting up **open source business accelerators** to provide open source developers with mentorship, community access, training, legal and licensing consulting, participation in open

[78] Such building blocks include common operating system distributions for servers, workstation and mobile devices, software for virtualisation and orchestration platforms, as well as software for network security including VPNs, supply chain security and compliance.

[79] The Eclipse Foundation supports industrial open source collaboration in the automotive sector through the Eclipse Software Defined Vehicle Working Group, which provides open governance, technical alignment and a shared development environment for automotive manufacturers, suppliers and technology providers working on software-defined vehicle building blocks.

[80] OpenRail Association.

[81] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2025) 270 final.

[82] The 2026-2027 Horizon Europe work programme already includes a support measure to support open source business models. This will be expanded under the new programming period.

standards development and related business development strategies, including marketing. Second, by leveraging the new instruments under the ECF, the Commission will consider supporting open source projects in moving to commercial level maturity, scaling adoption through an ecosystem of providers and integrators. The actions proposed on public procurement will also help open source vendors, integrators and providers reach anchor customers.

Supporting open source stewardship

Open source steward organisations (such as foundations providing legal, financial and organisational support for specific projects and communities) are widely recognised as effective governance structures to make projects viable and flourish over time. Open source building blocks are mostly maintained through foundations[83] with US (and Chinese) big tech providing a massive share of the funding and contributions[84]. At EU level, the **Cyber Resilience Act (CRA)** recognises open source foundations as 'stewards' of projects and acknowledges their role in keeping infrastructure secure and reliable. By creating a special regime with defined responsibilities, the CRA can act as a stimulus to set up such foundations. The CADA also caters for the establishment of foundations in the fields of cloud and AI in the EU.

The Commission will increase the EU footprint in the governance of open source stewards and foundations. It will do so in collaboration with the Member States, via the EDIC on Digital Commons, the European open source communities and the private sector. Specific measures to this end include:

- Developing a **'stewardship toolkit'** (on legal set-up, branding, interface usability, business models) for the establishment of associations/foundations in the EU;
- Identifying priority areas/sectors and **financial support for creating steward organisations**, as proposed in the CADA Regulation;
- Supporting the **establishment of a European Digital Public Infrastructure Steward Organisation**, in close cooperation with the Digital Commons EDIC and the eID open source communities. The aim is to provide a single EU-anchored home to govern strategic open source assets developed or co-funded by the EU, beyond code stewardship and reference framework implementation and conformance. This Steward Organisation could also serve as a channel to feed in experience in implementing European assets into European and international standardisation processes;
- Launching a **feasibility study on establishing an EU-level framework** that would identify the most suitable measures the Commission could implement to enable European foundations/associations to be governed by a single set of rules across the single market;
- Amplifying the voice of open source communities and their representativeness in the public space and supporting the set-up of professional **association(s) for open source contributors**.

Maintaining and securing open source code

[83] Foundation Directory – FLOSS foundations.

[84] Europe makes a sizeable upstream contribution to foundational open source components, but this contribution is uneven and often not matched by structured, long-term maintenance capacity. In core infrastructure, such as the Linux kernel, EU-headquartered firms remain visible upstream contributors. In Linux 6.15, SUSE and Linutronix (Germany) contributed 3.8% and 2.0% of changesets respectively, Jonathan Corbet, 'Development statistics for the 6.15 kernel', LWN.net, 26 May 2025.

Open source projects, including projects working on critical components that power our digital infrastructure (e.g. operating systems distributions, web servers, VPNs, containers, etc.), often draw on voluntary work carried out by developers. They often suffer from a lack of stable funding, solid infrastructure and governance. Maintaining code quality and security requires securing resources and continuity to attract contributors for a long period of time. Uncertainty about the maintenance of open source projects affects their credibility and long-term viability and may constitute a severe security vulnerability. Importantly, the EU's digital infrastructure rests on a set of non-EU chokepoints, the disruption of which would cascade rapidly into banking, healthcare, transport and government services.

In coherence with the EU Preparedness Union Strategy and its work on minimum preparedness requirements for vital societal functions, the Commission will support the security and integrity of critical components as well as the trust in open source solutions, through a combination of measures to:

- expedite the development of voluntary security-attestation programmes under Article 25 of the Cyber Resilience Act (CRA) and **create a voluntary EU assessment framework for open source**, attesting compliance of the solutions with key EU security rules and providing a qualitative assessment;
- build on the concept of dependency analysis under the CRA, by creating, with the support of ENISA, a **list of most exposed open source software and infrastructure dependencies**[85];
- create an **'Open Source Maintenance Instrument'** for supporting the maintenance and security upkeep of essential components, creating a European capacity and capability to fork projects;
- support, with the help of ENISA, a **strategic contingency programme setting up mirroring and build capabilities,** including for source code and software packages, to ensure continued access where there are the most critical and security-relevant dependencies;
- promote the **use of trustworthy AI in experimental settings, such as support to self-healing mechanisms** that improve the swift detection and secure remediation of vulnerabilities in open source software;
- support efforts to **increase the security of AI-generated open source code**, as the trade-off between development speed and security may introduce a high rate of inherent design flaws that could lead to systemic vulnerabilities.

Skills

Schools and universities often mostly use proprietary solutions to train students, support teachers and manage education data. This has allowed large tech companies to capture European schools and higher education institutions. To improve the skills needed to use open stacks and develop and contribute to open technologies, the Commission will support:

- **master programmes on collaborative open source development**, on integrating open source software skills, community governance and sustainability models, following successful precedents in the Digital Europe programme;

[85] Under the CRA, concerned actors generate Software Bills of Materials for their products; even if these are not published, they can be requested by market surveillance authorities and used by the Administrative Cooperation Group (ADCO), with the support of ENISA, to perform an EU-wide dependency assessment.

- **learner mobility, under the 2027 Erasmus+ programme**, to develop awareness and expertise in open source principles and methodologies, and cooperation partnerships amongst organisations to promote the use of open source solutions;
- **skills training for civil servants** on open source and digital interoperability by further expanding the training provided by the Interoperable Europe Academy[86].

4.3. Promoting open and interoperable digital ecosystems for public administrations

The public administrations' ability to act confidently in the digital domain as well as to enforce and implement policies increasingly depends on their capacity to control, understand and shape the technologies on which it relies. For public services and policies, open digital technologies can be the practical basis for technological sovereignty and long-term resilience: the ability to build, maintain and adapt digital systems in line with European values, regulatory frameworks and operational needs.

Over the past years, the Commission has built solid foundations for open digital technologies. The 2020 **open source software strategy** initiated a cultural shift ('think open')[87], clarified rules for software distribution[88], and triggered an expansion of inner-sourced and open sourced components. The creation of the Open Source Programme Office (OSPO), the launch of code.europa.eu[89], the EU Open Source Solutions Catalogue[90], and community-building initiatives such as hackathons, bug bounties, the OSPO Network, have significantly increased adoption and visibility of open source and open technologies across Commission departments and in public administrations across Europe. The Commission's Open Source Observatory[91] further strengthens this ecosystem by nurturing a broad community, sharing best practices and raising the profile of open source solutions developed and used by public administrations.

The Commission has launched initiatives that already illustrate this approach, including a sovereign real-time communication platform based on the **Matrix** protocol and a collaboration environment based on **openDesk**. It will also test laptops powered by alternative operating systems amongst its staff. Other examples include the deployment of open source networking solutions such as **OpenVPN** to support secure connectivity services and the widespread use of **Drupal** across more than 300 europa.eu websites. This approach is supported by the new **Cloud Sovereignty Framework**[92], which sets eight concrete sovereignty objectives and minimum assurance levels to enable cloud providers to demonstrate compliance with European standards, values and EU law. These initiatives are part of the Commission's action plan to advance its technological sovereignty and sovereign cloud procurement.

National strategies and public policies increasingly refer to **open source as a strategic tool.** Member State public administrations increasingly adopt open source software to manage sovereign digital infrastructures.[93]

---

[86] This is the Commission's free online learning hub with the courses tailored to the public administration context along with reusable training materials that organisations can adapt in their own system.
[87] The aim of the Commission's open source strategy 2020-2023 (C(2020/7149 FINAL) is 'to reinforce an internal working culture that is already largely based on the principles of open source'.
[88] Commission Decision C(2021)8759 on the open source licensing and reuse of Commission software.
[89] About code.europa.eu.
[90] EU Open Source Solutions Catalogue.
[91] Open Source Observatory (OSOR).
[92] Cloud Sovereignty Framework | European Commission.
[93] France with La Suite, and Germany with OpenDesk, provide collaborative tools for public administration, while Estonia uses the open source X-Road as the data exchange layer for its national digital government services.

In addition, the launch of the **European Digital Infrastructure Consortium (EDIC) on Digital Commons** (under the initiative of France, Germany, Italy and the Netherlands) shows a clear commitment to deploy, maintain and scale Digital Commons across Member States that is fully in line with the Commission's vision for open source.

However, the **evaluation of the 2020 strategy** and the results of the **call for evidence** indicate persistent structural challenges in both EU bodies and national public administrations. The challenges include uneven code publication practices, limited operational and legal guidance, security and sustainability constraints, insufficient coordination and reuse across administrative levels, and continued dependence on proprietary solutions in strategic areas.

The public sector as an anchor customer for open source solutions

Unlike in other world regions, such as the US, open source providers, in particular SMEs, have a structural disadvantage in the implementation of **procurement** in the EU, where specifications in individual tenders have historically been designed around the characteristics of proprietary vendors and focus on bundles of services and itemised prices rather than total cost and overall value, including public policy goals. They make limited mention of open standards and models and the necessary in-house skills[94].

This situation tends to favour incumbent suppliers and tolerate vendor lock-in[95]. An open source first principle in the purchase and procurement of software by public administration could revert this trend. The proposal for CADA promotes the use of open source components released under an open source licence and introduces the measures needed to reduce dependencies from proprietary solutions. In addition, it promotes the sharing and reuse of open source licence software published in a catalogue or repository, connected to the EU OSS Catalogue.

In this context, the Commission will **support EU public authorities in incorporating open source in the preparation and evaluation of their software procurement procedures** by:

- developing, building on the experience of Member States[96] and on the upcoming review of the public procurement rules and the CADA, guidelines and best practices on:
    i) drafting calls for tenders for the procurement of software that include open standards, specifications and models and allow open source solutions to compete with proprietary solutions;
    ii) evaluating bids based on open source solutions;
    iii) drafting calls for innovative partnerships for open source alternatives including provisions for prototypes and maintenance[97];
- promoting the participation of open source developers in policy labs shared by practitioners and policymakers to increase both contribution of open source experts into policymaking and awareness and compliance with EU policies.

[94] Examples include calls for tender that are designed around features of proprietary solutions, favouring single-vendors, and focusing on an assessment of immediate costs rather than a longer-term cost-benefit analysis. In addition, the requirements for the size and turnover of the bidders often excludes SMEs which would be the vast majority of OSS companies. See: CADA IA Study; 'The open source way to EU digital sovereignty and competitiveness', 2025 European Alliance for Industrial Data, Edge and Cloud; Open source roadmap on cloud, Open source initiative; Euro-stack Position paper on EU procurement for Open source digital sovereignty, 2025.
[95] CADA impact assessment study, stakeholder consultation.
[96] Deutschland-Stack.
[97] For example; Programme « Alternative »: un DCE structurant pour bâtir une trajectoire souveraine et open source au service des établissements de santé | CAIH - Centrale d'Achat de l'Informatique Hospitalière.

A reference model for public administrations

Achieving an open digital ecosystem that is sovereign by design **requires tackling three questions**: what is built and operated in the ecosystem, who sustains it and how are choices steered over time? The Commission proposes a strategic framework based on three mutually reinforcing pillars: **trusted digital assets** (their maturity, security and reliability), **capabilities and communities** (the skills and collaborative networks that sustain them), and **governance and investment** discipline (the decision-making that steers technology choices and spending over time).

The Commission, guided by the 'public money, public code' principle and in line with the **Interoperable Europe Act** and the CADA, will prioritise openness, the need to boost resilience, interoperability and long-term technological control, while not excluding the use of other solutions where security, confidentiality or legal constraints require it, following a pragmatic risk-based approach. It will focus on **strategic areas** such as **secure communication**, **digital workplace services**, **software development stacks** and **collaborative development environments**, as well as **data** and **AI** capabilities.

Trusted assets, services and guidance

A resilient open digital ecosystem for public administrations requires secure, well-maintained digital assets and services that can be confidently adopted, shared and reused across organisational boundaries. Trusted open assets enhance **strategic control over the Commission's digital stack** and are a necessary precondition for sovereignty, security and long-term sustainability. The Commission will also work to bring together **the technologies and practices required to develop and maintain trusted open digital assets at scale**. This work will seek to overcome the structural challenges that public administrations face when adopting open source and open technologies. In this context, the Commission will:

- draw up a coherent set of operational guidance consolidating existing legal, security, architectural and technical practices for adopting, developing and publishing open digital assets and services;
- strengthen the **Open Source Programme Office** and **EU Public Sector OSPO Network** and relevant mechanisms under the **Interoperable Europe Act** as central hubs for guidance and organisational learning, including compiling a catalogue of services that support the adoption, development and publication of open digital assets; Member States are also encouraged to give their OSPOs advisory tasks with regard to public procurement processes;
- enhance the visibility, reuse and strategic resilience of open digital assets to improve discoverability and systematic reuse across Commission departments, EU bodies and Member States;
- cooperate with European Digital Infrastructure Consortia (EDICs) such as IMPACTS and the Digital Commons EDICs and other groups to jointly identify and develop key open digital assets (such as DCAT-AP);
- develop and enforce common security baselines for the Commission's open source code repositories covering security monitoring, vulnerability management, licence compliance and automated dependency risk detection.

In parallel, the Commission will support experimentation by expanding the **Open source Labs**, a testing environment managed by the OSPO where Commission departments can test and evaluate open source solutions for public administrations.

Empowered communities

A thriving open digital ecosystem for public administrations depends on communities and networks that collectively create, maintain and evolve shared knowledge, assets and services. Open source communities, alongside open-science networks, standards bodies, data stewardship initiatives and GovTech innovators, constitute a critical layer of Europe's digital capacity. Public administrations play a key role not only as users of digital solutions but also as contributors to shared Digital Commons. In this context, the Commission will:

- Strengthen its internal communities[98] and develop skills in open collaboration. It will integrate open digital ecosystem competencies for the public administration into training and professional development programmes and highlight meaningful contributions to open source, open data, open science and standards development in its recognition mechanisms.
- Enable structured and secure participation in European open ecosystems for the public administration clarifying and simplifying rules for participation in external open source and open knowledge communities. It will step up cooperation with other EU institutions and Member States through a structured EU OSPO Network within the Interoperable Europe Community.
- Expand engagement with innovation communities both at European and global level.

Strong governance and decision-making

A sustainable open digital ecosystem for the public administration requires predictable rules, aligned incentives and coherent decision-making structures. Strategic digital choices must consistently support long-term control, interoperability, transparency, security, and public value.

Without a clear alignment across investment, policy design and evaluation mechanisms, there is a risk that openness and sovereignty considerations are applied inconsistently. Stability and predictability in decision-making are essential to embed open digital ecosystem principles across a public administration's activities. To provide clarity and long-term strategic direction, governance and investment processes will be progressively aligned with openness and sovereignty-by-design principles. In this context, the Commission will:

- embed the goals of openness and sovereignty-by-design in digital investments and project lifecycles by integrating structured assessment criteria into governance checks and maturity frameworks to ensure that control, interoperability, portability and sustainability considerations are systematically evaluated from the earliest design stages;
- review and update the digital-ready policymaking framework to further integrate openness, interoperability and sovereignty considerations, and encourage open source reference implementation, ensuring that legislative and strategic initiatives promote reusable, interoperable and transparent digital solutions.

4.4. Reinforcing digital technological standards and international outreach

One of the key objectives of the EU's international digital strategy[99] is to step up economic and business cooperation with partner countries. The EU aims to deepen and broaden its partnerships for example through Digital Dialogues, Digital Partnerships, and an integrated **EU**

[98] These may include an inter-DG network of Commission representatives to exchange practices and coordinate activities related to open source and open technologies, as well as interinstitutional cooperation with other EU institutions / bodies.
[99] JOINT(2025) 140 final, endorsed by Council Conclusions on 20 Nov 2025.

Tech Business Offer. This initiative supports EU companies and innovators in providing technology services to public and private entities in partner countries. The Pact for the Mediterranean is rolling out the EU Tech Business Offer in the southern Mediterranean. The Global Gateway offers the opportunity to advance digital partnerships, digital policy dialogues and digital investments in the EU and partners' interests, with a leading role for the private sector.

The EU, taking a Team Europe approach[100] , will **support EU open source developers and innovators** to deploy their solutions in enlargement and partner countries. It will also support cooperation with local open source communities and encourage the uptake of EU solutions, including open source solutions globally. It will promote EU-grown open source solutions ready to be reused, adapted and implemented in partner countries in key areas such as the Open Internet Stack, AI and software, the Digital Identity and Business Wallets. This will strengthen Europe's role as a leader in open source digital tools, aligned with EU values. At the same time, it will maintain open international collaboration with all developers and projects that are aligned with EU values and the objectives of this strategy.

Integrate open source processes into standard setting processes

The pervasiveness of open source in critical areas such as cybersecurity, AI and internet technologies makes it critical to ensure that developments in this field are adequately reflected in digital **standardisation** processes. The foundational standardisation work required by EU law, such as the CRA and the AI Act, will need a structural engagement of the open source communities to provide technical input and help deliver high-quality standards.

In the upcoming revision of the EU Standardisation Regulation, the Commission will propose measures to **improve cooperation between open source and standardisation communities**. It will do so by better integrating open source processes and communities into standard setting processes, providing conditions to make certain standards implemented in open source, and by providing sufficient funding to support the overall objective of improving legal certainty and swift availability of high-quality standards that support EU legislation and policy priorities.

4.5. Monitoring framework

The measures listed above in the open source strategy are designed to leverage the power of open source to increase control over critical areas of the EU digital infrastructure. By mitigating vendor lock-in, increasing transparency, security, and accountability, they can bolster European autonomy without retreating into isolation.

To ensure that above measures have a tangible, substantive impact on the open source ecosystem in Europe, the Commission will monitor implementation according to the timeline of the actions and based on the monitoring framework described in (Annex I).

Implementation of the measures will span several years, depending on the specific level of complexity and underlying funding source for each measure. To ensure that they continue reflect the state of the art and remain in line with European tech sovereignty objectives, the Commission will discuss progress annually with the Member States in the **Digital Decade Board**, along with the actions needed at national and EU level to meet this strategy's goals. Based on those discussions, the Commission will report to the European Parliament every three years.

[100] I.e., joint action by the EU, its Member States, the European Investment Bank and the European Bank for Reconstruction and Development.

5. Conclusions

The *technological sovereignty package* marks a pivotal step towards **the EU's goal of technological sovereignty while preserving its openness to the world.**

The measures it contains promote a **rapid shift from *reactive* action on resilience and risk mitigation to *assertive* and *proactive* action.** By tackling critical dependencies, fostering homegrown innovation and leveraging open strategic partnerships, the EU can transform its technological vulnerabilities into strengths, ensuring that its digital future is both sovereign and sustainable.

The package includes four initiatives: the **Chips Act 2.0**, the **Cloud and AI Development Act**, the **open source strategy**, and the **Digitalisation and AI in Energy Roadmap**. These form a cohesive framework, together with existing initiatives, to move towards the goal of creating a 'European technology stack'. To achieve this goal, the package sets out measures to boost the EU's capacity throughout the value chain, boost trust in Europe's digital ecosystem by ensuring openness, (cyber)security and resilience, and manage technological interdependence by leveraging (trusted) partnerships. At the same time, it aims to underpin the European approach to technological sovereignty by taking a human-centric approach that upholds EU values.

Mainstreaming the goal of technological sovereignty across the EU's growth strategy requires **a true 'ecosystem approach'.** This means combining in a strategic and concerted manner demand-side measures, supply-side measures, support to strategic projects that pursue the same goals and decisive action to create the needed enabling conditions. These include mobilising investments, both public and private, simplifying the digital single market rulebook, and developing the skills needed. The EU must balance openness with autonomy and ensure its technological base remains competitive, secure and values driven.

Member States are invited to translate the initiatives set out in the technological sovereignty package into national action, notably through the December 2026 revision of their National Digital Decade Strategic Roadmaps. In doing so, they should take due account of the recommendations issued in the framework of the State of the Digital Decade.

The stakes are high. Without decisive action and swift implementation, Europe risks falling further behind in the global tech race. Therefore, this package is not just a policy framework: it is a **strategic imperative to future-proof Europe's economy, security and sovereignty**.