EUROPEAN
COMMISSION

Brussels, XXX
[…](2026) XXX draft

SENSITIVE*
UNTIL ADOPTION

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

* Distribution only on a 'Need to know' basis - Do not read or carry openly in public places. Must be stored securely and encrypted in storage and transmission. Destroy copies by shredding or secure deletion. Full handling instructions https://europa.eu/!db43PX

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 lying 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, technological dependencies are becoming strategic liabilities. This is especially true as structurally higher and rising energy costs in Europe are holding back its competitiveness, particularly in energy-intensive technologies like cloud or AI. In a world of rapid technological acceleration and intensifying strategic rivalry, the EU thus risks a structural erosion of its industrial and technological base, unless it acts decisively to close its innovation gap. **This calls for an accelerated shift in the EU's posture from a *reactive* focus on resilience and risk mitigation to an *assertive* and *proactive* strategy grounded in technological sovereignty**.

***Technological sovereignty* refers to Europe's ability to develop, control and scale its critical technologies, infrastructure, services, and data, including its digital ecosystems, that underpin its economy, security and society, while resisting foreign interference.** This requires[2] to: i) boost homegrown industrial capacity and autonomy at each step of the supply chain of digital technologies, progressing towards a full European technology stack, while increasing the choice for end users in the Digital Single Market; ii) secure the supply of digital technologies underpinning Europe's competitiveness also by diversifying away dependencies particularly on a single or a limited number of non-EU suppliers, including via trusted partnerships; iii) gain control over data infrastructures and critical data, while developing the capacity to effectively leverage them; and iv) set the standards for key strategic technologies.

Technological sovereignty remains grounded in openness, partnership, and fair competition and does *not* equate isolation, protectionism, or tech decoupling. A technologically sovereign Union should effectively manage global technological interdependence. Strengthening Europe's technological base and independence in key digital supply chains –especially where other technology powerhouses[3]– creates strategic counterweights that enhance Europe's capacity to remain open to the world, without compromising its interests and values. This is how the EU can be both **sovereign and cooperative** going forward: a reliable and predictable partner, committed to deepening trusted relations, and forging new, mutually beneficial technology partnerships with those who 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 in advancing the EU's technological sovereignty while preserving its openness to the world. It builds on existing initiatives that the EU has put forward as policy and regulatory foundations of a coherent framework for asserting technological sovereignty: the **Competitiveness Compass**[5] identifies closing the innovation gap, decarbonising the economy, and reducing strategic dependencies as transformational imperatives for EU

[1] The Draghi report on EU competitiveness. 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] Relearning_the_Language_of_Power_GETF.pdf
[4] The EU Tech Business Offer | Shaping Europe's digital future
[5] COM(2025) 30 final

competitiveness; the **Communication on strengthening the EU's economic security**[6] offers a framework and a toolbox to achieve economic security, from investment screening to export controls to anti-coercion policy; the **Joint Communication on an International Digital Strategy for the European Union**[7] 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**[8] and related **ApplyAI Strategy**[9] put Europe on the path to becoming a true AI continent, by coordinating investment 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 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**[10], to strengthen Europe's semiconductor ecosystem and supply chain resilience including measures to boost domestic demand for chips;
- 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 third countries;
- a **Strategy for EU Open Digital Ecosystems ('Open source Strategy')**, included in this Communication, to reinforce Europe's autonomy across the whole stack as well as in the public administrations and EU Institutions by leveraging open source software; and
- a **Delegated Regulation** and **Strategic Roadmap for Digitalisation and AI in Energy** to underpin the sustainability of European data centres and avoid 'greenwashing' in this area.

Mainstreaming the goal of technological sovereignty at the heart of the EU's growth strategy requires acting on the right levers (Section 2) and following a true 'ecosystem approach' (Section 3) - leveraging the EU's research excellence, 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, 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 and of their geoeconomic implications. Europe remains heavily reliant on non-EU suppliers for raw materials, and renewable energy technologies, as well as for key elements of advanced digital infrastructure including semiconductors, cloud computing, and essential AI hardware and solutions –and continues to import specialized software, electronic components, and manufacturing inputs 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 translate into geopolitical vulnerabilities, a risk that Europe can no longer ignore. In fact, the past few years have seen a stark increase in the use of export controls, limitations to foreign direct investment and to outbound investments, sanctions and other restrictive measures being routinely deployed by third countries, including directly or indirectly against the EU and its Member States, with serious consequences on the EU's growth and stability.

[6] JOIN(2025)977 final
[7] JOIN(2025) 140 final
[8] COM(2025)165 final
[9] COM(2025)723 final
[10] COM(2022)45 final

High market concentration and vendor lock-in by a few non-EU players across the technology stack, including software, 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 tangibly impact Europeans' lives, affecting the industrial production of cars, healthcare equipment, energy infrastructure and consumer goods across the Union.

Despite sustained efforts under the **European Chips Act**[11], the EU produces only **around 10% of global semiconductors** and is dependent on the US and East Asia for both mature and advanced nodes, including AI chips that are indispensable for core European industrial ecosystems but also for the next generation of strategic capabilities. As **for cloud computing infrastructure and services,** failing to capture the gains of the first digital revolution led by the internet led to a slower digital adoption across the EU economy and society and to a **heavy dependence of the EU on foreign providers.**[12] 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 foreign jurisdictional data reach and surveillance, creating material risks to public order.

The Package addresses these challenges by acting on **two mutually reinforcing levers**:

A. Securing Europe's supply chains via an open strategic autonomy approach;

B. Reinforcing the 'European way' to technological sovereignty.

2.1 Lever A: Securing Europe's supply chains via an open strategic autonomy approach

A first sub-lever is moving towards a "European technology stack", strengthening the EU's capacity throughout the value chain. To address investment gaps, scaling barriers and skills shortages, Europe must reinforce its ability to develop, deploy and operate its own critical technologies –from advanced semiconductor design and manufacturing to cloud infrastructure and AI as well as to digital technologies for space and defence. Without sufficient own capacity, Europe cannot close its competitiveness gap, reduce dependencies, or shape global technological standards. This will also include promoting the EU tech business offer abroad.. For instance, the Global Gateway strategy offers a framework to scale-up investments and partnerships in digital transformation where EU security and competitiveness are the highest and where they meet our partners' interests.

The actions under the **Open source Strategy** fit very well with this objective – aiming to promote open European alternatives across the stack. Likewise, **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 **EuroHPC**[13], a world-class data and computing infrastructure financed by the EU and Member States, governed by EU rules, and serving EU priorities. With the **AI Factories**[14] **initiative,** it has now evolved into an AI-

[11] The European Chips Act has 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 Union's advanced R&I capabilities and their industrial exploitation.

[12] While the EU cloud services market is growing, the market share of EU providers decreased from 29% in 2017 to 15% in 2022 and has remained stable since – leaving over 70% of the market in the hands of three US hyperscalers.

[13] The European High Performance Computing Joint Undertaking (EuroHPC JU)

[14] AI Factories | Shaping Europe's digital future

optimised infrastructure, with **19 AI Factories**[15] and 13 AI Factory Antennas gradually becoming operational across Europe. In addition, **sovereignty is at the core of the value proposition of AI Gigafactories (AIGFs)**[16] – for which 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, boosting Europe's scientific capabilities and industrial competitiveness. Yet, for industry, academia, and public administrations to migrate their most sensitive workloads, they must be certain that strategic data and proprietary models remain under exclusive EU oversight. AIGFs thus ensure autonomous control over core physical and digital infrastructure and must be resilient against external dependencies and immune to extraterritorial 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 sub-lever is boosting trust in Europe's digital ecosystem by ensuring its openness, (cyber)security, and resilience. In a digital environment marked by growing market concentration and vendor lock-in, especially of non-EU providers, cybersecurity must be safeguarded across the technology stack, while interoperability, portability, and widespread adoption of open standards ensure that public and private users can choose, switch and scale technological solutions without prohibitive costs. **CADA** will promote open source, secure and sovereign solutions. It complements the **Data Act**[17], which mandates industry-driven common specifications put forward in two draft Implementing Regulations to improve interoperability and portability when switching cloud providers. The **Open source Strategy** also promotes secure, transparent and auditable open source ecosystems for critical systems and digital infrastructures. **CADA** and the **Open source Strategy** build in this respect on the framework developed through the **revised text of the EU Cybersecurity Act**[18] which creates a certification and risk-management framework that can effectively limit the role of high-risk vendors in critical digital infrastructure. In parallel, the **EU Digital Identity**[19] and **EU Business Wallet**[20] aim to establish sovereign and interoperable digital identity systems, reinforcing trust and enabling secure digital interactions across borders.

A third sub-lever is effective management of technological interdependence leveraging (trusted) partners, including for supply-chain diversification purposes. In a context of 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 third countries for key digital technologies, while retaining effective regulatory and operational control where critical infrastructure, sensitive data or essential public services are concerned. This is especially the case where the EU is heavily reliant on third country technologies, such as AI chips, cloud services, and the underlying stacks. For instance, the recent semiconductor shortages[21] demonstrate how supply disruptions

[15] AI factories are publicly supported AI infrastructure centres that provide shared supercomputing resources and datasets, often offering free or subsidized compute access to universities, startups, and SMEs to accelerate AI research and innovation.
[16] EU launches InvestAI initiative to mobilize €200 billion of investment in artificial intelligence
[17] Regulation - EU - 2023/2854 - EN - Data Act - EUR-Lex
[18] EUR-Lex - Ares(2025)2970891 - EN - EUR-Lex
[19] European Digital Identity - European Commission
[20] COM(2025)838 final
[21] 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.

can translate directly into tangible impacts on daily life, affecting industrial automotive production, healthcare equipment, energy infrastructure and consumer goods across the Union, 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 reinforce the security of supply for semiconductors by reducing strategic technological dependencies. **CADA** introduces an obligation for governments to conduct sovereignty risk assessments, with the view to improve resilience, the protection of public order and boost European sovereign alternatives where appropriate – while putting an end to 'sovereignty-washing'.

2.2 Lever B: Reinforcing the 'European way' to technological sovereignty'

A first sub-lever is sustainability of innovation and investments, whereby digital technologies support decarbonisation, while contributing to addressing high energy prices. Technological innovation and independence are in fact closely intertwined with the green transition. The rapid expansion of digital infrastructure, including data centres, is hugely increasing energy demand across Europe. By fostering the deployment of energy-efficient cloud infrastructures, **CADA** will respond to these needs by ensuring that the deployment of new data centre capacity is aligned with sustainability goals and strategic planning, helping to prevent additional pressure on constrained 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 Union's climate and energy goals. The **Strategic Roadmap for Digitalisation and AI in the Energy Sector** will support the rapid and large-scale deployment of EU digital and AI solutions in key areas for decarbonisation – e.g. electrification of industry, transport and households; improved system integration across adjacent sectors; electricity grid optimisation; energy efficiency in buildings and industry; and development of demand-side flexibility. A **Delegated Regulation on the sustainability of data centres** will establish a common EU scheme to rate the sustainability of data centres in Europe through electronic labels issued by a European database –increasing transparency on their environmental performance and supporting the deployment of more sustainable digital infrastructure EU-wide.

A second sub-lever is adopting a human-centric approach that upholds EU values such as safety, security, inclusivity, and accessibility, in line with the **European Declaration on Digital Rights and Principles**[22]**, as well as safeguarding the level-playing field underpinning competition, empowerment and participation.** These values are embedded in the EU digital legislations, underpinned by evidence-based assessment and adopted by the EU democratically elected institutions Technological innovation is not just a driver of economic growth. It is also a **cornerstone of Europe's just and societal transition**. Therefore, the EU must ensure that digital advancements actively strengthen democratic resilience, solidarity, and freedom of choice, for instance by offering trusted and harmonised public digital infrastructure across the EU. In this package, **CADA** promotes the build-up of data centres and the development of a sovereign cloud and AI stack for the whole Union addressing freedom of choice and inclusion. The assessment framework proposed by the Open source Strategy would recognise solutions that fit with the EU values and comply with EU regulations. The objectives of the Package are aligned with the goals of the **Digital Services Act (DSA)**[23] which promotes transparency, accountability and user rights, ensuring that also in the digital space fundamental

[22] European Declaration on Digital Rights and Principles | Shaping Europe's digital future
[23] Regulation - 2022/2065 - EN - DSA - EUR-Lex

rights are respected while curbing the spread of illegal content, and with the **Digital Markets Act (DMA)**[24] which promotes fair business practices, market openness and innovation.

2.3 Horizontal enablers

In addition to acting on these two interlinked levers of technological sovereignty, the EU must act upon key horizontal enablers of technological sovereignty: an agile **regulatory and business environment**, including simplification, cutting red tape, and reducing administrative burden, as well as adequate **skills** and sufficient **financial firepower** for Europe to achieve technological sovereignty.

The Commission is simplifying Europe's digital rules so that businesses can spend less time on paperwork and more time on innovation within the Digital Single Market. The Union's Digital Single Market rulebook is now composed only of a few horizontal acts covering AI, Data, Platforms, Telecom and Cloud. For instance, the **Digital Networks Act**[25] will replace the European Electronic Communications Code[26], the BEREC Regulation[27], the Radio Spectrum Policy Programme[28], and core parts of the Open Internet Regulation[29]. In the area of data, the Data Governance Act[30], the Free Flow of Non-Personal Data Regulation[31], and the Open Data Directive[32] have been repealed and key provisions inserted into a consolidated **Data Act**[33]; in addition, targeted amendments were introduced to the GDPR to ensure that more data can be lawfully used for training AI in Europe, thus bringing legal certainty on its application. The **Digital Omnibus**[34] introduces a series of targeted changes to ensure the effective application of the rules in the **AI Act**[35]. The **European Business Wallet**[36] will simplify business operations, regulatory compliance, and cross-border interactions for companies.

Skilled workforce is crucial to the competitiveness and resilience of the EU's digital ecosystem. The Package aims to boost the development of specialised skills in the fields of semiconductors, cloud and open source, building on the **Digital Decade Policy Programme**[37] priorities. These include upskilling and reskilling the existing workforce, supporting transitions from declining sectors, strengthening advanced education and training in emerging technologies, and enhancing the attractiveness and mobility of students and workers, including from outside the Union, in STEM fields. Equipping individuals and businesses with the necessary digital skills for the EU's digital economy is also a central objective in the **2025 European Skills Agenda**[38]**.**

Finally, achieving sustained financial firepower is a crucial step to support the sizeable investments needed to be technologically sovereign. Europe must mobilise strategic investment to scale innovation, deploy critical infrastructure and support the growth of

[24] Regulation - 2022/1925 - EN - EUR-Lex
[25] EUR-Lex - Ares(2025)4545535 - EN - EUR-Lex
[26] Directive - 2018/1972 - EN - eecc - EUR-Lex
[27] Regulation - 2018/1971 - EN - EUR-Lex
[28] Decision - 2012/243 - EN - EUR-Lex
[29] Regulation - 2015/2120 - EN - EUR-Lex
[30] Regulation - EU - 2023/2854 - EN - Data Act - EUR-Lex
[31] Regulation - 2018/1807 - EN - EUR-Lex
[32] Directive - 2019/1024 - EN - psi directive - EUR-Lex
[33] Regulation - EU - 2023/2854 - EN - Data Act - EUR-Lex
[34] EUR-Lex - 52025PC0837 - EN - EUR-Lex
[35] Regulation - EU - 2024/1689 - EN - EUR-Lex
[36] EUR-Lex - 52025PC0838 - EN - EUR-Lex
[37] Decision - 2022/2481 - EN - EUR-Lex
[38] European Skills Agenda - Employment, Social Affairs and Inclusion

homegrown technology champions. This requires leveraging public funding more effectively and reducing fragmentation across financial instruments and national markets. The **proposal for the 2028–2034 Multiannual Financial Framework (MFF)**[39] has been designed with three objectives in mind: to be more focused, more impactful, and better equipped to address current structural weaknesses and rigidities. Within this framework, the **European Competitiveness Fund (ECF) and its Digital Leadership Window** are a central vehicle to steer and leverage investments towards technological sovereignty, covering the full investment continuum - from collaborative research to innovation, and industrial and infrastructure deployment and to supporting innovation ecosystems and their scaling up and resilience, including support to advanced skills. Operating as a dedicated investment capacity, the ECF aims to strengthen European competitiveness in critical technologies and strategic sectors. It will also act as a powerful enabler, by using budgetary instruments to crowd in private, institutional and national investments across the entire digital value chain, including targeted measures for start-ups, scale-ups and SMEs. Beyond its direct investment role, coherence is ensured with Horizon Europe (FP10) and complementary instruments, notably the **National and Regional Partnership Plans (NRPPs)**. Through them, technology sovereignty efforts can be reinforced at Member State level, aligning with common competitiveness priorities and enabling coordinated support for key areas and projects of strategic European interest.

As public funding alone cannot close Europe's investment gap – estimated in the Draghi report at EUR 800 billion annually – it is essential to crowd in massive volumes of private capital. Europe must address urgently its structural shortage of private risk capital for high-growth and deep-tech companies. The **InvestAI programme**[40] aims to mobilise EUR 200 billion in AI and illustrates the scale of investment needed to support our technological ambitions. The **Scale-up Europe Fund**[41] and **Industrial Accelerator Act**[42] further contribute to this goal by facilitating industrial scale-up and improving access to financing for innovative companies. By aligning financial resources with strategic technological priorities and targeting investment where market failures are the greatest –from frontier technologies and secure digital infrastructure to skills and industrial capacity.

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

Achieving EU technological sovereignty requires **developing a new 'ecosystem approach'** acting across the entire value chain and combining multiple instruments: i) demand-side measures; ii) supply-side measures and support for Strategic Projects; and iii) action reinforcing horizontal enablers.

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. This 'ecosystem' approach responds to a strategic necessity: measures reducing supply dependencies and boosting domestic capacities in Europe must go hand-in-hand with measures creating demand in downstream sectors – in line with the levers of boosting open strategic autonomy and reinforcing the 'European way'. In turn, this link is strengthened by attracting foreign champions to Europe through adequate competitiveness enablers, such as innovation,

[39] EU budget 2028-2034
[40] EU launches InvestAI initiative to mobilise €200 billion of investment in artificial intelligence | Shaping Europe's digital future
[41] Commission partners with private investors to set up multi-billion Scaleup Europe Fund
[42] Carriages preview | Legislative Train Schedule

favourable cost factors, skills, and sufficient financial firepower in support of Strategic Tech Projects EU-wide. No other strategy is likely to deliver the same results.

The abovementioned ecosystem approach is clearly reflected in the various initiatives of this Package, including the **Chips Act 2.0**, **CADA**, and the **Open source Strategy** presented in Section 4. The sections below show how the different elements of the package come together among themselves and vis-a-vis other past and ongoing initiatives such as AIGFs.

3.1 Demand-side measures

While the **Chips Act** included mostly supply-side measures, the **Chips Act 2.0** will act also on the demand side. New studies suggest that the European semiconductor demand could double by 2040, driven primarily by consumer electronics, automotive, energy and data centres. Among these sectors, data centres are projected to experience the most significant growth in consumption demand. Additionally, demand shows growth across all node ranges, with sub-16 nm nodes exhibiting the steepest increase, 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 new data centres and cloud-related measures under CADA. This is in line with a stack-based approach – from hardware to software – to contributing to Europe's technological sovereignty.

Each AIGF will in fact operate at industrial scale – having 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 by linking suppliers with users via offtake agreements and a demand forum. It will also support collaboration on custom chip design with industry involved early in development. To stimulate demand and support EU-based start-ups and scale-ups, the Chips Act 2.0 will deploy **public innovation procurement,** as a strategic tool, creating a clear and structured pathway to purchasing semiconductor technologies developed in the Union. A **cybersecurity risk assessment** will evaluate both technical vulnerabilities and non-technical factors in anticipation of the revision of the Cybersecurity Act. Finally, **grand challenges** will help generate early demand and facilitate faster market entry for semiconductor technologies developed in the Union.

CADA's measures to accelerate the deployment of data centre infrastructure acts as a demand-side measure for the Chips Act 2.0. CADA also defines four levels of cloud sovereignty services based on criteria linked to the control over the service, control over the supply chain, the processing of AI inference data, the location of the infrastructure and the level of cybersecurity. Member State will need to carry out a sovereignty risk assessment to establish which use cases in their administrations require which sovereignty level, while the Commission will issue guidelines to support them in their assessment. CADA will also foster the EU value added of public spending in the area of cloud and AI. The CADA grand challenge to reach autonomy across the cloud and AI stack will be linked to the development of processors and accelerators, which are designed and, where appropriate, manufactured in the EU.

Finally, the **Open source Strategy** promotes the adoption of open source solutions by the public and private sectors, to reinforce EU sovereignty. Priority is given to solutions that are already mature and that can establish themselves as genuine alternatives or as new markets. In particular, the implementation of the European Business Wallet and the EU Digital Identity Wallet, which are based on open source, offer significant opportunities 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 reinforce Europe's mainstream and advanced semiconductor capacity, 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, including a Union-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 scope of the Chips Act provisions on **first-of-a-kind facilities** will also be clarified 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 and enable its application to Strategic Projects. The Commission will seek to simplify and accelerate procedures for the assessment of projects, for instance by considering national support schemes for smaller aid amounts to be assessed on aid intensities. These efforts reflect the Commission's commitment to reducing administrative burden and increasing speed and legal certainty, which is particularly critical in the fast-moving semiconductor sector to strengthen Europe's competitiveness.

The Chips Act 2.0 also emphasizes the **acceleration of the industrialisation of pilot lines**, transforming successful pilot manufacturing facilities into commercially viable manufacturing capabilities. It also **adds photonics and photonic-integrated circuits as an additional component of the Chips for Europe Initiative**[43], as they are key enabling technologies for a wide range of strategic sectors, including telecommunications, data centres, AI, sensing, healthcare, automotive and quantum.

CADA introduces a framework that simplifies and harmonises data centre deployment EU-wide. The goal of the regulation is to triple EU capacity in the next 5-7 years and reach the Union's needed capacity by 2035, while ensuring high sustainability standards and balanced geographical deployment across Member States. It introduces cloud and AI challenges to develop a complete AI and cloud stack.

CADA also includes a mechanism to identify and support Strategic Projects, for instance prioritising support for data centres with significant built-in innovation and sustainability or that contribute to the balanced distribution of computing capacity. As illustrated with the beta-launch of the EU age verification app, communities of developers can stress-test open source solutions, de-bug them and make them more robust. The Open source Strategy includes actions and Strategic Projects to turn mature open source building blocks into widely used solutions across the tech stack, and to develop new ones in areas where dependencies exist, such as operating systems or AI algorithms. This is to be coupled with an **Open source Maintenance Instrument** and a voluntary assessment framework for open source to increase security.

3.3 Enablers

In terms of **investment needs** for boosting the EU's semiconductor ecosystem, the Commission estimates and additional **EUR 120 billion** in public and private investment by 2035, of which around **EUR 30 billion** for the EU-wide advanced semiconductors manufacturing foundry. Expanding data centre capacity will require the mobilisation of around **EUR 200 billion**, mostly of private origin, by 2036[44], with the research and innovation initiative foreseen under the CADA requiring around **EUR 2 billion over the next 7 years** at

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

the EU level. To address the immediate need for investments responding to rapid market and policy development, in particular regarding the convergence of cloud, edge, AI and network technologies, a **targeted amendment** of the **Smart Networks and Services Joint Undertaking** broadens its scope, complementing CADA. To cover the full spectrum of measures under the Open source Strategy, it is estimated that an envelope of a **EUR 1 billion euros** will need to be mobilised by the public and private sectors over the next seven years. Finally, to support the implementation of the Strategic Roadmap for Digitalisation and AI in Energy, it is estimated that around **EUR 20 billion** should be mobilised by public and private investors.

Private investors must also have good visibility over the investment potential across the Union, for the newly unlocked investments to produce the most value added for the European tech ecosystem. This is why the Commission will develop an **EU-level promotion initiative targeting streamlined access to information regarding the investment needs and readiness**. Information regarding investment needs and readiness will be accessible to investors from the EU and third countries alike. This 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 CADA, and highly innovative ecosystems assisting the implementation of the Apply AI sectoral flagships (for example the "Autonomous Drive Ambition Cities").

As regards the other key enabler of **regulatory simplification**, the **Chips Act 2.0** sets up provisions ensuring that semiconductor technology facilities and Strategic Projects qualify for accelerated environmental approvals under the EU's fast-track permitting rules. Secondly, building up 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, **CADA** aims to accelerate data centres deployment by harmonising investment conditions, focusing on sustainability and innovation. Within designated areas, operators will have simplified access to land, reliable energy infrastructure, and funding opportunities across the Union.

Finally, in terms of **skills development**, building the specialised ICT skills necessary for EU tech sovereignty requires coordinated governance across public authorities, industry, academia and training providers, with due regard to regional specificities. At Union level, priorities include upskilling and reskilling the existing workforce, supporting workers transitioning out of declining sectors, and strengthening advanced education and training in emerging technologies - particularly in semiconductor-related professions. Equally critical is enhancing the attractiveness of STEM fields and fostering the mobility of students and workers, including talent from outside the Union, to ensure Europe can compete and innovate at the frontier of the global digital economy.

4. A Strategy for EU Open Digital Ecosystems: Leveraging open source to strengthen Europe's technological sovereignty ('Open source Strategy')

Open source[45] is a key lever to achieve the Union's technological sovereignty as it is often underpinning critical communication, commerce, healthcare or government services. Europe, the birthplace of Linux, is home to a strong and vibrant community of over 3 million open source contributors, delivering digital solutions aligned with European principles and values[46,47]. This ecosystem is key to boosting Europe's competitiveness by accelerating innovation, lowering technology costs, reducing dependence on foreign vendors, and enabling local companies, researchers, and governments to build secure, customizable, and globally competitive digital solutions.

However, at present, **the EU spends EUR 264 billion annually mostly on US' proprietary IT products and services**[48]. This creates dependencies that affect Europe's ability to control key digital infrastructures, reduce lock-in risks, and ensure security and compliance[49]. **Europe's strong open source capabilities offer a path to avoid this dependence**. Yet, the EU's open source ecosystem faces several challenges: lack of sustained funding after the early stage of a project, uncertainty regarding maintenance, accessing capital for scaling-up, low brand recognition, and barriers in public procurement. Additionally, as global open source ecosystems are increasingly shaped by non-EU actors, notably the US and, in an increasingly strategic manner, China, Europe must bring in the international scene not only code and talent but also vision and leadership.

While existing EU legislation and policy already provide support for open source[50], this **Open source Strategy** sets out four objectives: i) leverage open source for tech 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. The Strategy includes **supply-side measures** to enable EU communities and companies to develop, scale up, maintain and secure high-quality open source components; and **demand-side measures** to accelerate the private and public sectors' adoption, integration and deployment of open source solutions.

[45] 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 (OSD), 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).

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

[47] 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.

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

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

[50] 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 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 1600 contributions to the Commission's Call for Evidence from a broad range of stakeholders detailed in Annex IV. 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 Union entities and public administrations EU-wide. This 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 responds directly 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 barriers to 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, enable communities and companies to jointly develop, adapt, and secure technologies. Open source is also a preferred approach for cybersecurity, as its transparency allows for public inspection.

Open source projects operate under various models: independent, volunteer-driven and informal networks, sometimes hosted by foundations; projects managed by large companies (mostly non-European), which use open source for their core products but add proprietary layers for monetisation; and dedicated "pure open source" companies that install, maintain and support. The growing success of open source as a business model is evident in the rise of promising EU-based companies with industrial grade capabilities[51]*. This industry is consolidating at national level with associations promoting these models at EU level*[52]*. Yet, nearly half of all code commits in Europe come from small firms with fewer than 50 employees, which continue to face structural barriers to scaling, branding, and market integration in procurement and industrial deployment*[53]*.*

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 I). However, while the EU has allocated 800 million EUR[54] *in the current MFF, this funding lacks strategic focus on long-term*

[51] **Odoo** (Belgium) recently reached a valuation of €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 relies on 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 decentralized communication, **XWiki** and **CryptPad** for collaboration, and **OpenNebula** for cloud and edge computing.

[52] For example, APELL – The European Open source Software Business Association - represents national open source business associations in 8 Member States (DE, DK, IT, FI, FR, NL, PT, SE).

[53] 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

[54] Including investments in NGI, Open Internet Stack, SIMPL middleware, open source related AI (e.g. openEuroLLM) and Cybersecurity, Risc V related investments

sustainability of open source solutions and communities, which is key to maintaining sovereign digital solutions over time.

4.1 Promoting and leveraging open source for EU technology sovereignty

To reduce dependencies from third countries based on an initial assessment of dependencies (Annex I), a targeted effort is required to boost promising areas that already offer alternatives and to address rapidly identified gaps in strategic domains. The Commission will collaborate with Member States and the private sector on: i) supporting existing open source sovereign alternatives; and ii) building European alternatives in critical technological areas.

Make available and facilitate adoption of existing EU sovereign alternatives

To support the deployment and uptake of existing open source solutions as sovereign alternatives, the Commission will:

- Scale-up the **Open Internet Stack**[55] to provide a unified catalogue, a one-stop shop for open source building blocks and sovereign solutions in Europe.
- **Increase awareness of available EU sovereign solutions,** including by mobilising existing 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[56] 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 interoperability, integration and reuse of open source stacks. This includes a Software Development Kit to support integration of the EUID into relying-party systems as well as an open source reference implementation protocol for legally valid communication channels for the EBW; 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 the implementation of the fully open source Age Verification solution in cooperation with the EUID open source communities.
- **Partner with Member States**, in particular with the European Digital Infrastructure Consortium (EDIC) on Digital Commons[57] to **facilitate the development and/or adoption of open source alternatives**. In the short-term, priority areas will focus on domains where EU open source alternatives are established, such as cloud infrastructure, digital workplace

[55] Under Horizon Europe Work Programme 2026-2027, the Commission has mobilized an investment of 41.3 million EUR through 3 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

[56] Such as the index developed by the Digital Resilience Initiative, https://thedigitalresilience.org/, or the Software Sovereignty Scale https://dri.es/the-software-sovereignty-scale

[57] 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.

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**, by supporting open and decentralised social media solutions and platforms. Presently, the Commission manages an instance of Mastodon, hosting the Commission's official accounts and it will expand the service to a broader range of users.

Build European open source alternatives to proprietary solutions

the Commission will promote open source solutions as the default approach in calls for proposals across R&I programmes, with the aim of building European alternatives based on open source to complete a full EU sovereign stack. This includes referring to open source and open models in calls and catering for the participation of open source communities through agile funding mechanism. Examples of key technology areas where open source developments could be prioritised include:

- **Semiconductors:** development, under the Chips Act 2.0, of open source hardware IP such as the one based on RISC-V; targeted investment in open source Electronic Design Automation (EDA) tools.
- **Operating systems:** computer operating systems; mobile operating systems, Internet of Things and robotics and drones 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**: focus on the development of open source AI models including state-of-the-art model architectures, foundational models, and agentic frameworks. In addition, 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 energy and automotive have already taken the lead to set 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 Union’s economic security and prosperity.

The Commission will also leverage open source in critical sectors of the economy to reduce dependencies from third countries, especially in AI, 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, healthcare and pharmaceuticals; robotics; manufacturing, or defence, security and space.
- Support **industrial collaboration** platforms, where competitors develop jointly open source building blocks[58] to create common software stacks. This increases the overall efficiency of digital transformation while maintaining competition, as seen in the automotive or railway sectors[59].

4.2. Strengthening and promoting a vibrant open source ecosystem

The EU can count on a strong ecosystem of developers, a nascent open source industry in key areas and new collaboration vehicles among Member States (e.g. EDICs such as the one on 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 efforts of EU developers.

Scaling up open source startups and open source business models

In line with the **EU Startup and Scale Up Strategy**[60], the Commission will **leverage EU programmes and public procurement** to help the transformation of open source initiatives into sustainable business. Firstly, the Commission will establish dedicated support actions[61] setting up **open source business accelerators** to provide open source developers with mentorship, community access, training, legal and licensing consulting, participation in open standards development and related business development strategies including on marketing. Secondly, leveraging the new instruments under the ECF, the Commission will support the transition of open source projects to commercial level, scaling adoption through an eco-system of providers and integrators. The proposed actions for public procurements will also contribute to provide anchor customers for open source vendors, integrators and providers.

Supporting open source stewardship

Open source steward organisations (such as foundations providing legal, financial, and organizational 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[62] with US (and Chinese) big tech representing a massive part of the funding and contributions[63]. At EU level, the **Cyber Resilience Act (CRA)**, recognising open source foundations as "stewards" of projects, acknowledges their role in keeping infrastructure secure and reliable. In addition, by establishing a special regime with defined responsibilities, the CRA can act as a stimulus for

[58] 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.

[59] https://openrailassociation.org/

[60] 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.

[61] Under Horizon Europe Work Programme 2026-2027 there is already a Support Action to support open source business models. This will be expanded under the new programming period.

[62] Foundation Directory - FLOSS Foundations https://flossfoundations.org/foundation-directory/

[63] 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

the set-up of these structures. The proposal for the Cloud and AI Development Act 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, in collaboration with the Member States, via the EDIC on Digital Commons, the European open source communities and the private sector. Specific actions include:

- Development of a **"stewardship toolkit"** (on legal setup, branding, interface usability, business models) for the establishment of associations/foundations in the EU.
- Identification of priority areas/sectors and **financial support for the establishment of stewards' organisations**, as proposed in the CADA Regulation.
- Support 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 governance home for strategic open source assets developed or co-funded by the Union, also beyond code stewardship and reference framework implementation and conformance. This Steward Organisation could also serve as a structured channel for European implementation experience to feed into European and international standardisation processes.
- Launch a study on the **feasibility of establishing an EU-level framework** that would identify appropriate measures the Commission could implement to enable European foundations/associations to be governed by a single set of rules across the Single Market.
- Strengthen the voice of open source communities and their representativeness in the public space, support the establishment of professional **association(s) of open source contributors**.

Maintaining and securing open source code

Open source projects, including those working on critical components that power our digital infrastructure (e.g. operating systems distributions, web servers, VPNs, containers, etc), often benefit from voluntary work from developers and suffer from lack of stable funding, solid infrastructure and governance. Maintaining code quality and security requires securing resources and continuity in attracting contributors over 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, transportation, and government services.

The Commission will support the security and integrity of critical components and enhanced trust in open source solutions through a combination of measures:

- Expedite the development of voluntary security attestation programmes pursuant to Article 25 of the Cyber Resilience Act (CRA) and **establish a voluntary EU assessment framework for open source**, attesting compliance of the solutions with key EU rules and providing a qualitative assessment.

- Building on the concept of dependency analysis under the CRA, the Commission, with the support of ENISA, will create a **list of critical and security-relevant open source software and infrastructure dependencies**[64].
- Establish an **'Open source Maintenance Instrument'** for sustained financial support for 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 capabilities** including for source code and software packages to ensure continuity of access, for the most critical and security-relevant dependencies.
- Promote the **use of trustworthy AI to support self-healing mechanisms** that enhance the timely 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 use proprietary solutions to train students. This has allowed large tech companies to capture European higher education. To improve the skills necessary to use open stacks and develop and contribute to open technologies, the Commission will support:

- the development of an **open source software suite for schools and universities**, and vendor-agnostic training, as proposed in the Cloud and AI Development Act.
- **master programmes on collaborative open source development**, Open source Software skills integration, community governance, and sustainability models, following successful precedents in the Digital Europe Programme.
- the **mobility of learners, within the Erasmus+ Programme 2027**, to develop awareness and expertise in open source principles and methodologies, and cooperation partnerships amongst organisations to promote the use of open source solution.
- the **development of skills among civil servants** in open source and digital interoperability by further expanding the offer of Interoperable Europe Academy[65].

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, they are the practical basis for digital 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 implemented important foundations towards open digital technologies. The 2020 **Open source Software Strategy** initiated a cultural shift ("think

[64] Under the CRA, concerned actors generate Software Bills of Materials (SBOMs) 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 a Union wide dependency assessment.

[65] This is the Commission's free online learning hub with the courses relevant to the public administration context along with reusable training materials that organisations can adapt in their own system

open")[66], clarified rules for software distribution[67], and triggered an expansion of inner-sourced and open sourced components. The creation of the OSPO office, the launch of code.europa.eu[68], the EU Open source Solutions Catalogue[69], 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 services and in public administrations across Europe. The Commission's Open source Observatory[70] 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 implementation of a sovereign real-time communication platform based on the **Matrix** protocol and of a collaboration environment based on **openDesk**. Further examples include the deployment of open source networking solutions such as **OpenVPN** to support secure connectivity services, the widespread use of **Drupal** across more than 300 europa.eu websites. This direction is also supported by the new **Cloud Sovereignty Framework**[71], which defines eight concrete sovereignty objectives and establishes 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 and Member States' public administrations increasingly adopt open source software to manage sovereign digital infrastructures.[72]

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** point to persistent structural challenges in both Union bodies and national public administrations, including uneven code publication practices, limited operational and legal guidance, security and sustainability constraints, and insufficient coordination and reuse across administrative levels, as well as continued dependence on proprietary solutions in strategic areas.

The public sector as an anchor customer for open source

Unlike in other world regions, such as the US, open source providers, in particular SMEs, have a structural disadvantage in **procurement frameworks** in the EU, where the procedures have historically been developed around the characteristics of proprietary vendors and focus on bundles of services and itemised prices rather than total cost and overall value, including public

[66] 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", https://commission.europa.eu/about/departments-and-executive-agencies/digital-services/open source-software-strategy_en

[67] Commission Decision on the open source licensing and reuse of Commission software https://ec.europa.eu/transparency/documents-register/detail?ref=C(2021)8759&lang=en

[68] https://code.europa.eu/

[69] https://interoperable-europe.ec.europa.eu/eu-oss-catalogue

[70] https://interoperable-europe.ec.europa.eu/collection/open source-observatory-osor

[71] Cloud Sovereignty Framework | European Commission

[72] 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.

policy considerations, while the consideration of open standards and models and the necessary in-house skills are limited.[73]

This situation tends to favour incumbent suppliers and tolerate vendor lock-in[74]. CADA aims to revert this trend by introducing an **open source-first principle in the purchase and procurement of cloud and AI software** by public administrations[75]. In addition, it promotes the **public money / public code paradigm** by asking public administrations to make the software they develop or purchase available for reuse. The recommendation accompanying CADA provides guidance in this respect.

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, in line with the upcoming review of the public procurement rules and with CADA, and building on the experiences of Member States[76], 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) evaluation of bids based on open source solutions; iii) drafting calls for innovative partnerships for open source alternatives including provisions for prototypes and maintenance[77].
- Promoting the participation of open source developers in policy sandboxes between practitioners and policy makers to increase both contribution of open source experts into policy making and awareness and compliance with EU policies.

A reference model for public administrations

An Open Digital Ecosystem, sovereign by design **requires action on three fronts**: what is built and operated, who sustains it, and how choices are 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).

As for the Commission, guided by the "public money, public code" principle and in line with the **Interoperable Europe Act** as well as CADA, it will prioritise openness, strengthening resilience, interoperability and long-term technological control, while not excluding the use of other solutions where security and confidentiality require it, following a pragmatic risk-based approach. Focus will be given to **strategic areas** such as **secure communication**, **digital workplace services**, **software development stacks** and **collaborative development environments**, as well as **data** and **AI** capabilities.

[73] Examples include calls for tender that are designed around features of proprietary solutions, favouring single-vendors, and focusing on the assessment of the immediate costs rather than over longer-term cost-benefit analyse. 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.

[74] CADA IA Study, Stakeholder consultation.

[75] Add reference to the specific CADA article when final

[76] https://deutschland-stack.gov.de/

[77] 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

Trusted Assets, Services, and Guidance

A resilient open digital ecosystem for public administrations depends on 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 constitute a necessary precondition for sovereignty, security and long-term sustainability**. The Commission will also work to **consolidate the technologies and practices required to develop and maintain trusted open digital assets at scale**. This work will address structural challenges that public administrations face when adopting open source and open technologies.

In this context, the Commission will:

- establish a coherent set of operational guidance consolidating existing legal, security, architectural and technical practices for the adoption, development and publication of open digital assets and services;
- strengthen the **Open Source Programme Office (OSPO)** and **EU Public Sector OSPO network** and relevant mechanisms under the **Interoperable Europe Act** as central hubs for guidance and organisational learning, including the definition of a catalogue of services supporting the adoption, development and publication of open digital assets;
- enhance visibility, reuse and strategic resilience of open digital assets, to improve discoverability and systematic reuse across Commission services, Union entities and Member States;
- collaborate 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 through reinforced **Open source Labs**, a testing environment managed by the OSPO where Commission services 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[78] and skills for open collaboration. Open digital ecosystem competencies for the public administration will be integrated into training and professional development programmes, and recognition mechanisms will highlight meaningful contributions to open source, open data, open science and standards development;

[78] 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.

- 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. Collaboration with other Union institutions and Member States will be strengthened through a structured EU OSPO Network within the Interoperable Europe Community;
- expand engagement with innovation communities 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 and public value.

Without clear alignment across investment, policy design and evaluation mechanisms, openness and sovereignty considerations risk being 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 openness and sovereignty-by-design in digital investment and project lifecycles 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 Policy Making framework to further integrate openness, interoperability and sovereignty considerations, and encourage open source reference implementations, 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 International Digital Strategy[79] is to enhance economic and business cooperation with partner countries. This is implemented through an integrated **EU Tech Business Offer**, which supports EU companies and innovators to provide technology services to public and private entities to such countries. The Global Gateway strategy offers the opportunity to advance digital partnerships, digital policy dialogues and digital investments in the EU and partners' interests, with a leading role for EU MS private sector.

The EU, through a Team Europe effort, will further **enable EU open source developers and innovators to deploy their solutions in partner countries as part of the EU tech business offer.** It will also further facilitate collaboration with local open source communities and encourage the uptake of EU solutions, incl. open source solutions, globally. It will promote EU-grown proprietary and open source solutions ready for re-use, adaptation and implementation in partner countries in key areas such as the Open Internet Stack, AI and software, or Digital Identity and Business Wallets. This will strengthen Europe's role as a leader in open source digital tools incl. open-source tools aligned with interests like security, privacy and transparency, while maintaining international collaboration open to all those developers and projects that are aligned with EU values and the objectives of this strategy.

Integrate open source processes into standard setting processes

[79] JOINT(2025) 140 final, endorsed by Council Conclusions on 20 Nov 2025

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 by better integrating open source processes and communities into standard setting processes**, providing conditions to make certain standards implemented in open source, and by ensuring adequate funding, supporting the overall objective of improving legal certainty and timely availability of high-quality standards that support Union legislation and policy priorities.

4.5. Monitoring Framework

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

The actions 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 and accountability, they can bolster European autonomy without retreating into isolation. The implementation will span several years, depending on their individual complexity and underlying funding source. To ensure that they continue reflect the state of the art and remain relevant to European tech sovereignty objectives, the Commission, will discuss progress annually with the Member States meeting in the Digital Decade Board, the actions necessary at national and European level necessary to deliver on this strategy's goals. Based on those discussions, the Commission will report to the European Parliament every three years.

5. Conclusions

The ***Technological Sovereignty Package*** marks a pivotal step in **advancing the EU's technological sovereignty while preserving its openness to the world, promoting an accelerate shift from a *reactive* focus on resilience and risk mitigation to an *assertive* and *proactive* approach.** By addressing 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 a "European technology stack" by strengthening the EU's capacity throughout the value chain, boost trust in Europe's digital ecosystem by ensuring its openness, (cyber)security, and resilience, and manage technological interdependence by leveraging (trusted) partnerships. At the same time, it also aims to reinforce European way to technological sovereignty, by adopting a human-centric approach that upholds EU values.

Mainstreaming the goal of technological sovereignty at the heart of the EU's growth strategy requires a true 'ecosystem approach' - leveraging demand-side measures, supply-side measures and support for Strategic Projects, as well as action on horizontal enablers such as mobilising investments, simplifying the Digital Single Market rulebook, and fostering the

development of adequate skills. The EU must balance openness with autonomy, ensuring its technological base remains competitive, secure, and values driven.

The stakes are high: without decisive 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**.