EUROPEAN
COMMISSION

Brussels, 16.6.2025
COM(2025) 290 final

ANNEX 1

ANNEX

to the

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions

State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future

{SWD(2025) 290 final} - {SWD(2025) 291 final} - {SWD(2025) 292 final} -
{SWD(2025) 293 final} - {SWD(2025) 294 final} - {SWD(2025) 295 final}

European Commission

State of the EU digital transformation in 2025: progress and horizontal recommendations

Contents

1. Introduction

This annex forms an integral part of the State of the Digital Decade 2025 report. It retains the four-chapter structure of the 2024 report, focusing on: technological sovereignty, security, and competitiveness; protecting and empowering people; harnessing digitalisation for the green transition; and a horizontal chapter on building coherence, efficiency and simplification.

The analysis provides an overview of the state of play, identifies key strengths to build on as well as gaps and shortages, and offers targeted recommendations to all Member States in areas requiring stronger collective action. The analysis primarily relies on the monitoring conducted through the Digital Economic and Society Index (DESI). It is further supported by relevant studies, expert analysis, and the National Digital Decade Strategic Roadmaps submitted by Member States.

2. Reinforcing technological sovereignty, security, and competitiveness

a. A continent supporting digital innovation and sovereignty

i. Closing the innovation gap

- *Research and Innovation (R&I) for a digitally transformed Europe*

The trends identified in the 2025 State of the Digital Decade are still very much demonstrating the EU's weakness in digital innovation, particularly the limited scale of **investment in R&D** and the insufficient focus on breakthrough innovation[1]. According to data from the EU Industrial R&D Investment Scoreboard, the US dominates digital R&D, accounting for around 40% of all digital companies and 53% of total R&D investment among those identified in 2023[2].

Overall, while Europe remains a global hub for scientific exchange, it **lacks critical mass** of top-performing players, reflecting a fragmented ecosystem with limited specialisation[3]. The latest available Eurostat data shows that the percentage of the ICT sector in gross value added is relatively low and grew only marginally in recent years, from 4.86% in 2019 to 5.46% in 2022[4]. While **European organisations excel in producing high-impact scientific publications, they struggle to transform this knowledge into patented innovation.** Compared to the US and China, **the EU lags behind in patent filings, with fewer applications submitted.**

Digital technologies also play a crucial role in the EU's efforts to innovate, compete and grow to ensure its freedom and reinforce its **security, strategic autonomy, and defence capabilities**, with a significant potential for leveraging synergies between civilian and defence applications. Start-ups and innovative companies in the field of dual-use technologies also play a key role, but their potential is limited by a long-standing defence investment gap—especially for deep tech and SMEs. Barriers like outdated policies and limited financing options further restrict growth.

To drive growth and cross-border investment in defence-related innovation, the European Commission has launched several dedicated instruments, including the EUDIS Matchmaking and Accelerator Programmes, and mobilised new funding channels through the European Innovation Council (EIC) and the TechEU Scale-up Fund. In January 2024, via the European Investment Fund, the Commission launched a EUR 175 million **Defence Equity Facility**, designed to leverage up to EUR 500

[1] Draghi, M., The future of European competitiveness, 2024, Part A – A competitiveness strategy for Europe.
[2] Joint Research Centre, Nindl, E., Napolitano, L., Confraria, H., Rentocchini, F., Fako, P., Gavinan, J. and Tuebke, A., The 2024 EU Industrial R&D Investment Scoreboard, 2024.
[3] Joint Research Centre, Eulaerts, O., Grabowska, M. and Bergamini, M., Weak signals in Science and Technologies - 2024, 2025.
[4] Source: Eurostat (Statistics | Eurostat). This indicator measures the importance of the ICT sector in the economy, reflecting the strength of the innovation ecosystems.

million in venture capital for defence technologies with dual-use potential. This complements European Defence Fund investments in advanced digital domains and innovation-driven initiatives. One of these initiatives is the EUDIS Hackathon, which gathered over 275 participants from 16 Member States and generated more than 70 innovative solutions to address pressing defence challenges.

Technological leadership - Recommended policies, measures and actions

R&I for a digitally transformed Europe

Member States should increase their public digital R&I expenditure, prioritising R&I investment in digital technologies that play a strategic role in the EU's competitiveness, resilience and sovereignty.

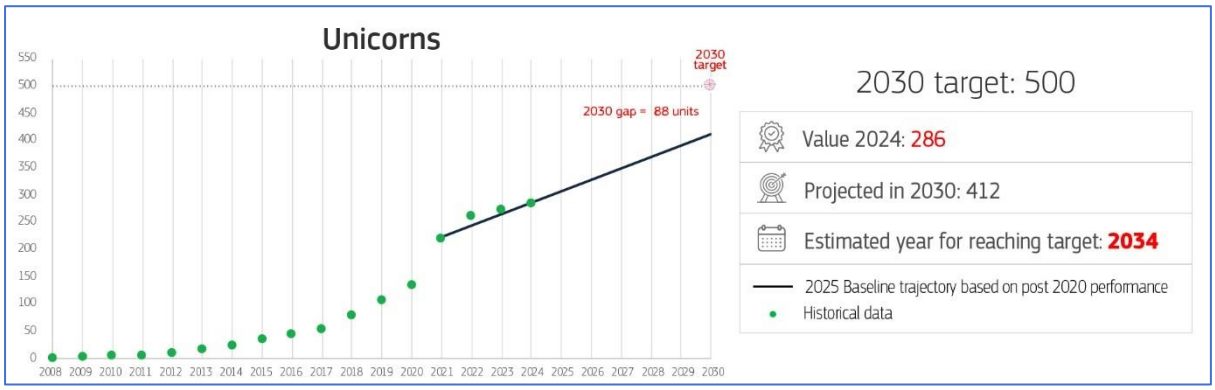
Harnessing digitalisation for EU's defence capabilities

Member States should:

- *strengthen their support to innovative actors, including start-ups proposing disruptive digital applications and services[5];*
- *boost the development of digital infrastructures that contribute to societal resilience in crisis contexts;*
- *better connect the defence and digital innovation communities, foster a new mindset towards preparedness and security culture across the digital sector, identify synergies between defence and digital programmes, investments, and applications.*

- *Boosting the scale-up capacity of Europe*

The 2025 data on **unicorns in the EU** reflects a slowing down of the dynamic that characterised COVID times in 2021 and 2022. **In 2024, the number of unicorns established in the EU rose by 12 units**, reaching 286 unicorns**.** The target of 500 unicorns is expected to be reached in **2034** if no further actions are taken[6].



There are significant variations among Member States – with Germany (69 unicorns), France (48) Sweden (39), and the Netherlands (32), topping the list. However, the EU still lags significantly behind China (397) and the US (1687), the latter demonstrating a higher annual growth rate (6% against 4.4% in the EU).

[5] In compliance with EU rules.
[6] European Commission based on Dealroom data.

Despite its vast economic potential, the Digital Single Market remains fragmented, with a complex landscape of national regulations, administrative procedures, and obstacles to data and knowledge sharing that leaves a large potential untapped.

First and foremost, there is a **need for a substantial development of EU capital markets**. The lack of private capital for 'big ticket' investments still prevails. This forces too many EU startups to seek late-stage growth capital from venture capital funds outside the EU, which can often result in them moving their corporate headquarters outside the EU. The **Savings and Investments Union**[7] will be crucial to improving how the EU financial system **channels savings into the real economy, and uses those savings for productive long-term investment**.

To foster the rise and development of scaleups, the EU is set to adopt an **EU Startup and Scaleup Strategy in 2025**. This strategy aims to address financial, regulatory, and administrative barriers that hinder startups from scaling up into mature, profitable companies–an urgent priority to prevent them relocating outside the EU. For innovative companies to emerge and existing ones to scale up, the **single market plays a crucial role**. As part of this effort, the Commission will present a **'28th regime'** to make it possible for innovative companies to benefit from a single, harmonized set of EU-wide rules, wherever they invest and operate in the single market. At the same time, the implementation of the **Digital Markets Act** is creating and opening up significant opportunities for startups and scaleups by imposing specific obligations on gatekeepers and thereby ensuring that small businesses that use such platforms benefit from fair and open markets.

However, EU-level action alone is not enough to address these challenges, and cooperation with Member States will be critical, especially to attract and retain talent, foster access to finance, promote tech transfer policies and the public procurement of innovative products and services. It can build on the Member State-led **Europe Startup Nations Alliance**[8] (ESNA), which supports national innovation policy makers in sharing and implementing best policy practices for startups.

Unicorns - Recommended policies, measures and actions

Member States should support coordinated action across the single market to address financial, regulatory, and administrative barriers and mobilise public policies tackling a comprehensive range of domains:

- *promote tech transfer, facilitate the creation of spinoffs from universities and research centres;*
- *mobilise public procurement budget to procure innovative products and services from startups;*
- *increase the amount and diversity of private capital (for example from national pension funds) available for co-investing in high-growth startups;*
- *identify and support tech innovators in their countries (e.g. identified through the innovation radar, or EIC or the Strategic Technologies for Europe Platform Seal of Excellence).*

[7] European Commission, Savings and Investments Union, A Strategy to Foster Citizens' Wealth and Economic Competitiveness in the EU, COM(2025) 124 final, 2025.

[8] Website: https://esnalliance.eu/.

ii. Fostering Ecosystems and infrastructure for an AI continent

Connectivity

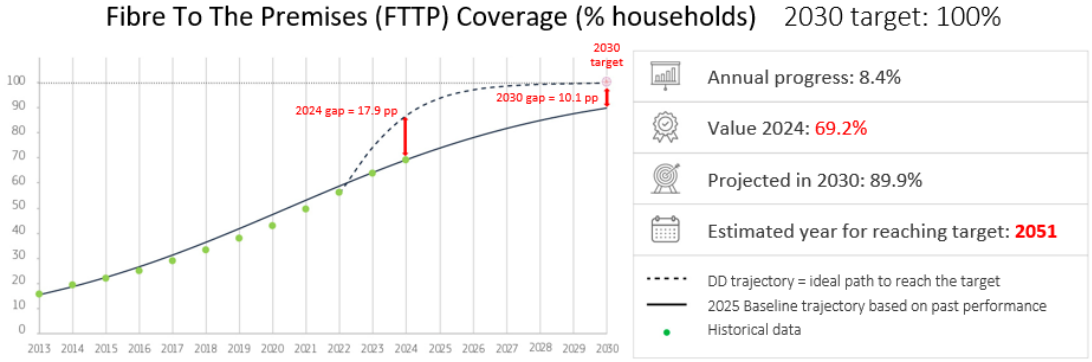
Modern connectivity is no longer a collection of separate technologies— satellites, submarine cables, mobile and fixed networks—but a deeply interconnected ecosystem. To respond to the growing demand for critical, low-latency applications, such as autonomous vehicles and remote surgery, higher amounts of data[9] need to flow seamlessly across all these domains, as disruptions in one can affect the entire network's performance and security. This requires a global approach, spanning from orbital assets to terrestrial infrastructures in a unified, resilient, and globally optimised system. The EU must already lay the the foundation for this approach, with full coverage of fibre and accelerated development of stand-alone 5G.

Regarding **fixed connectivity**, accelerated action is needed to meet 2030 targets. Very high Capacity Networks (VHCN) coverage reached 82.5% in 2024, with a growth rate of 4.9%, while fibre coverage stood at 69.2% of households in 2024, marking an 8.4% annual increase. However, at the current pace, **full coverage would only be achieved by 2051.** In particular, rural deployment of fibre lags behind, with just 58.8% coverage in 2024.

Data on the uptake of gigabit connectivity and 5G shows an upward trend, although there is still room for improvement. In 2024, only 22.3% of fixed broadband subscriptions were at speeds of 1 Gbps or higher (up from 18.5% in 2023). Overall, basic 5G coverage[10] across the EU reached 94.3% in 2024, which is comparable to the 97% estimated coverage in the US and 95% in China and India[11]. Rural 5G coverage in the EU and in the US are comparable with the EU at 79.6% and the US at 82%. Both regions have lower rural coverage compared to China (85.2% estimated) and India, which leads with 92.1% rural coverage. 5G take-up (share of the population using 5G SIM cards) increased in the EU from 21.7% to 35.6% in 2024. This is higher than India's 11.1%, but **it is still significantly behind the US** (96.5%) and China (73.1%). **Ensuring that the spectrum needs for future connectivity are met is another critical challenge,** while the incomplete assignment of the three 5G pioneer bands and the slow progress reported (on average in Europe only 75% of the relevant spectrum has been assigned by February 2025) exacerbate the problem.

In 2025, Europe is significantly falling behind in adopting 5G stand-alone (SA) networks, with only 2% of 5G users connected via SA infrastructure[12]**.** This sluggish uptake reflects ongoing challenges in infrastructure deployment and device readiness across the region. In stark contrast, the **US is far ahead** with **24% of its 5G users operating on SA networks** and **China has surged with 77.1%** — underscoring the country's aggressive roll-out of next-generation core technologies. These disparities reveal a growing global divide in 5G evolution, spotlighting China's technological momentum and exposing the structural and policy hurdles hampering Europe's shift from 5G non-stand-alone (NSA) to true SA capabilities.

[9] Statista, 2025 (Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2023, with forecasts from 2024 to 2028).
[10] The current KPI for the 5G target does not reflect the actual quality of service experienced by users. It monitors areas where a 5G signal is available, regardless of the network performance. The current stage of 5G deployment can be considered only as "basic 5G".
[11] All relevant statistics related to 5G can be found at the Commission's 5G Observatory website: https://digital-strategy.ec.europa.eu/en/policies/5g-observatory.
[12] Ookla. Omdia. A Global Evaluation of Europe's Digital Competitiveness in 5G Standalone, 2025.



In their **National Roadmaps**, Member States reported devoting a significant portion (approximately 28%) of their measures' total budget **to gigabit fixed connectivity**, amounting to EUR 80.6 billion (with EUR 56.6 billion coming from private sources). The 103 measures primarily focus on regulatory actions to facilitate network deployment, as well as financial support for non-viable and commercially unattractive areas and strategic parts of the networks. About one third of the measures are dedicated to each of the two areas. In their roadmap adjustments, Member States maintained a strong emphasis on regulatory actions to facilitate network deployment.

In terms of **5G investments**, Member States reported investing EUR 5.9 billion (with EUR 2.9 billion coming from non-public funds), which accounts for approximately 2% of the total budget of their measures. The 39 measures for 5G focus on **spectrum management**, as well as financial support for non-viable and commercially unattractive areas, and strategic parts of the network. There is equal emphasis on each of the two areas. In their roadmap adjustments, Member States placed a significant focus on increasing financial support for 5G networks.

To improve market incentives to build the digital networks of the future, the Commission is working on a future **Digital Networks Act** (DNA), to be proposed by the end of 2025, aiming to improve digital connectivity for all end-users. In parallel, the Commission is setting up 5G standalone **large-scale pilots** with EUR 205 million funding under the **Connecting Europe Facility**, a large-scale pilot for Telco-edge-cloud deployments under Horizon Europe (EUR 75 million funding), as well as taking a proactive role in the **global race for 6G** by developing a spectrum roadmap and shaping global standards.

Regarding **satellite connectivity (broadband internet, direct-to-device or D2D and Internet of Things or IoT satellite)**, the EU is facing a dual challenge of capacity and sovereignty. The EU remains heavily reliant on non-EU actors to access space, notably SpaceX launchers, and on **US satellite constellations such as Starlink,** while the satellite capacity of EU operators lags behind its competitors. Comparing the number of satellites paints a stark picture for the EU which has only 3 893 launched and planned satellites. China has launched 220 satellites and has an additional 27 198 planned, and the US has 7 633 launched and additional 33 397 planned - both countries have very ambitious expansion plans for the coming years[13]. Satellites are becoming an essential component of an efficient, secure and resilient connectivity network, increasingly providing low latency broadband connectivity. The convergence of non-terrestrial and terrestrial networks is accelerating, including in 5G and future 6G systems, increasing mobile coverage through satellite D2D connections—and improving network resilience and security with advanced encryption.

[13] Detecon International GmbH, Study on Mobile satellite services (MSS) in the 2 GHz band in the EU, 2025.

Already counting on GOVSATCOV, the EU will start improving its strategic presence in space with the development of IRIS². IRIS² is the new EU multi-orbit satellite constellation[14] of 292 satellites which will provide for secure connectivity and high-speed broadband to eliminate connectivity dead zones. In December 2024, the Commission and the SpaceRISE industry consortium, comprising the three major EU satellite operators, signed a 12-year concession contract for the design, development, and operation of IRIS². On the regulatory side, the Commission continues work with the Radio Spectrum Policy Group (RSPG) to develop a **common approach** to define common requirements for **satellite constellations** accessing the EU market and satellite D2D and to explore the potential of the EU harmonised 2 GHz Mobile Satellite System (MSS) frequency band, which will become available for reassignment in 2027, as a strategic tool to support its ambitions in the space market.

Submarine data cables are the backbone of global digital communication, carrying over 99% of international data traffic, which makes their security and resilience a top priority for the EU. In 2025, the EU has taken several steps to mitigate potential vulnerabilities that could be exploited by geopolitical adversaries (see section on cybersecurity below) and invested considerably in studies and works supporting submarine cables and backbone infrastructure. CEF-Digital already supports 51 Global Gateways projects (mostly on submarine cables) for a total investment of EUR 420 million. The demand for CEF funding is constantly increasing for submarine cables: the total requested funding is almost 6 times higher than the available budget in forth call.

Connectivity infrastructure - Recommended policies, measures and actions

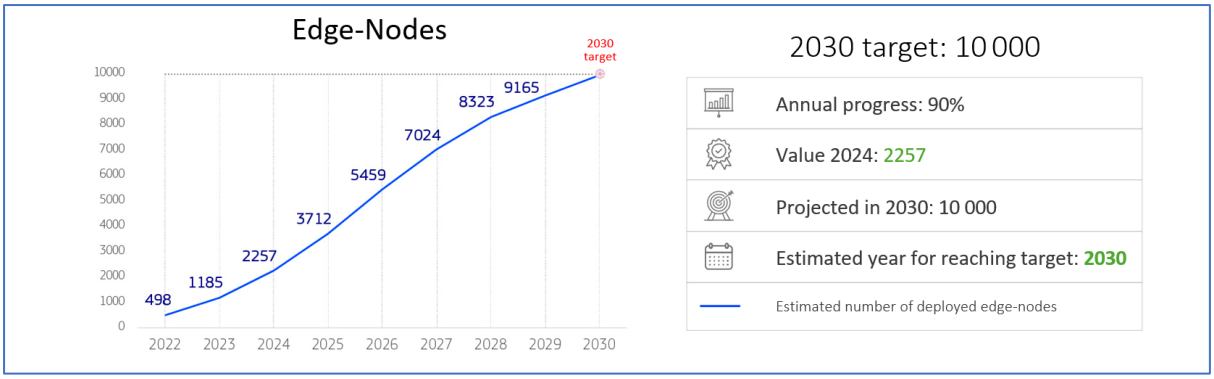
Member States should:

- *introduce targeted measures to accelerate fibre roll-out and take-up by end-users;*
- *use regulatory and financing measures to incentivise the densification of 5G networks, also based on EU-harmonised mm-wave spectrum, and accelerate the deployment of secure 5G stand-alone networks, including by fostering cross-border collaborations and promoting innovative use cases;*
- *support coordinated action for planning and developing a reliable, sovereign and resilient network of digital infrastructures and capacities, encompassing backbone terrestrial, submarine and satellite networks, across the EU and with international partner countries.*

Cloud and edge infrastructures

The role of **edge nodes is critical in the future AI ecosystem**. Edge computing enables more immediate AI processing of massive data volumes and intelligent interpretation of data in minimal processing times (milliseconds). It also provides a more secure processing environment and reduces data transmission costs and network congestion. The applications are numerous, including video observation, analysis and asset/equipment monitoring, tracking and performance optimisation[15].

[14] Meaning covering low Earth orbit (LEO), medium Earth orbit (MEO) and geostationary Earth orbit (GEO).
[15] Edge Observatory for the Digital Decade, Edge Deployment Data report 1, 2023.



In 2024, it is estimated that a total of **2 257 edge nodes** were deployed across the EU, which is a single-year increase of **1 072 new nodes** compared to 2023. 2025 represents a pivotal moment in the deployment trajectory; it is expected to see 1 455 new nodes deployed, the biggest single year increase, which is in line with the estimated trajectory to reach 10 000 by 2030. The density of edge nodes across the EU reveals varying levels of deployment across Member States. France, Germany, Italy, and Spain are at the forefront of edge node deployment. Today's edge node deployments mainly address the critical need for accessing real-time data, with 20% of organisations already using these solutions extensively and 42% planning to adopt them. As AI and machine learning applications evolve, businesses are likely to adopt edge nodes more with a promising future adoption rate of 54%[16]. This underlines the transformative potential of AI and machine learning in driving business innovation, informing decision-making, and monetising edge solutions.

Growing data centre capacity across Member States will also be critical in supporting the development of AI. The amount of computing power utilised to train leading AI systems has expanded by 350 million times over the past 13 years[17] and, since 2010, the training computing power used to create AI models has been **growing at a pace of 4.6 times per year**[18], underlying the dependence of AI on cloud computing infrastructure and software to train and use AI models at scale[19]. **The investment needs for developing cloud infrastructures are massive**. Europe today has **around 8-10 GW of installed data centre capacity, amounting to roughly a third of the installed capacity in the US** and half of the installed capacity of China[20]. Even though Europe's capacity is projected to increase significantly, potentially reaching 70% growth by 2030, the gap with the US is expected to widen further, as US data centre capacity is set to double in the same period[21]. Industry forecasts predict that demand for data centre services will outpace supply, widening the gap in Europe's cloud computing capacity relative to global competitors[22].

In this context, **the EU Cloud and AI Development Act** will be key to accelerate the deployment of data centres in Europe, by **cutting red tape**, accelerating permitting procedures, improving access to land, finance and energy, and creating the right conditions to incentivise large investments in energy-efficient cloud and edge capacity. The act will address these obstacles, with a **view to at least tripling the EU's data centre capacity within the next five to seven years and bringing it to a level that meets the needs of EU businesses and public administrations by 2035**. Finally, several Member States of the

[16] Edge observatory for Digital Decade, Edge Deployment Data Report – 3rd report, 2024.
[17] Lennart Heim, Markus Anderljung, Emma Bluemke, Robert Trager, Centre of the Governance of AI, "Computing Power and the Governance of AI", 2024.
[18] EPOCH AI, Notable AI models, 2025.
[19] OECD (2023) "A blueprint for building national compute capacity for AI", OECD Digital Economy Papers, No. 350, OECD Publishing, Paris.
[20] Hintemann, R.; Hinterholzer, S.; Progni, K. (2024a). Data centes in Germany - Current market developments 2024. Berlin: Bitkom e.V. Retrieved from Bitkom e.V. website: https://www.bitkom.org/Bitkom/Publikationen/Studie-Rechenzentren-in-Deutschland.
[21] Ibid.
[22] An upcoming study will consolidate these figures and provide DG CNECT with more granular data on capacity and needs, today and in 2030.

Joint European Forum for IPCEI (JEF-IPCEI) in November 2024 decided to enter into the **design phase of two new potential Important Projects of Common European Interest (IPCEI)**. These new initiatives, focused on innovative AI Services (IPCEI-AI) and on deploying computing infrastructure (IPCEI-ECI), amongst others to support the ambitions set out in the AI Continent Action Plan[23].

Moving forward it will be crucial for the EU to closely monitor the **deployment of data centre capacity across Member States** in cloud and edge infrastructures. Ensuring a balanced and strategic expansion of data centres is essential to supporting the growing demand for AI compute capacity. In practice, it will be fundamental to include the **systematic monitoring of investments in infrastructure and data centres.** This would help ensure that European businesses and the public sector have adequate access to the necessary compute capacity to benefit from edge, cloud computing and AI-driven solutions.

Cloud and edge infrastructure - Recommended policies, measures and actions

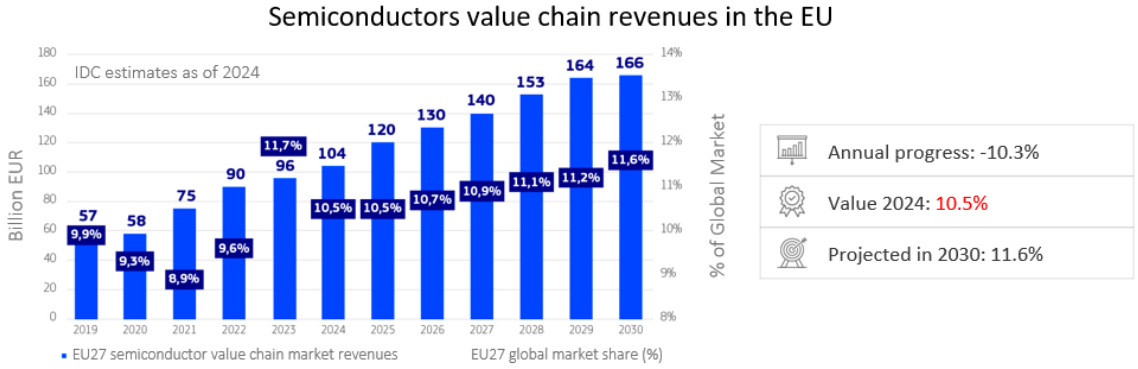
Member States should:

- *support the deployment of secure and sustainable cloud and edge nodes and focus national efforts on infrastructure-targeted investments and strategies to ensure that businesses have access to the sovereign compute infrastructure required for serving their cloud and AI needs.*
- *closely work with the Commission on the upcoming Cloud and AI Development Act, aiming to at least triple EU data centre capacity within the next five to seven years and bringing it to a level that matches the demands of EU businesses and administrations by 2035. This is an objective that could become a new Digital Decade target.*
- *engage fully with the Commission in the discussion on the outcome of the study supporting the Cloud and AI Development Act to establish methods for assessing and tracking the EU cloud compute infrastructure capacity.*

Semiconductors

In 2024 the **EU's share of global value chain revenues was 10.5%, still far from the 2030 target of 20%.** Huge investments were approved in the last semester of the previous US administration, and China is accelerating its investment in legacy chips manufacturing. The EU's share is projected to increase again moderately in the coming years driven by the steady growth of the EU's value chain revenues, in a context of sustained massive investments in other regions of the world, responding to strong growth of the global market revenues now projected to pass EUR 1.4 trillion in 2030. This implies that the EU's semiconductor revenues must grow more than four times their current value to achieve the Digital Decade target by 2030.

[23] AI Continent Action Plan, COM(2025) 165 final.



In their National Roadmaps, **Member States have committed to investing a substantial EUR 49.2 billion** in semiconductors, accounting for 17% of the roadmaps' total budget across all targets. Private sources are expected to contribute EUR 8.6 billion to this investment[24]. The 52 measures reported in the roadmaps mainly focus on supporting R&D and boosting production capacity and industrial deployment of semiconductors. Roughly one-third of the measures are dedicated to each of these areas, indicating a balanced approach to driving growth and innovation. These areas also remain a priority in the Member States' roadmap adjustments.

The **European Chips Act** has established a framework to attract investments from major semiconductor manufacturers into a first-of-a-kind for EU facilities. The first seven projects announced already exceeding EUR 30 billion in investments and there are other promising projects worth almost another EUR 30 billion in the pipeline. The approved IPCEI on Microelectronics and Communication Technologies (IPCEI ME-CT) brings together 14 Member States and 56 companies, channelling around EUR 20 billion from both private and public sources into 68 collaborative projects across multiple countries. Furthermore, a proposal for new IPCEIs on advanced semiconductor technologies is currently in the design phase. Moreover, the Chips Act is the basis for supporting five pilot lines with a total of EUR 3.7 billion funding. These projects will bridge the gap between laboratory innovation and industrial-scale manufacturing in key areas such as beyond 2nm leading-edge system-on-chip, fully depleted silicon-on-insulator applications, advanced packaging, wide band gap materials, and photonic integrated circuits.

For Europe to compete globally in the semiconductor sector, **it is essential to substantially increase investments and to continue its commitment to the leading value chain areas,** including semiconductor equipment, chips design, analogue components, sensors, photonics, while also securing a strong entry into emerging markets such as computing and AI-oriented silicon.

With this aim in mind, the Commission is starting the formal review of the Chips Act, which is planned by Q3 2026, with a clear support for a Chips Act 2.0 from industry, some Member States, and other stakeholders.

[24] Please note that measures included in the national roadmaps might draw on existing funding programmes and might include investments under the IPCEI mentioned in this paragraph.

Semiconductors - Recommended policies, measures and actions

Member States should:

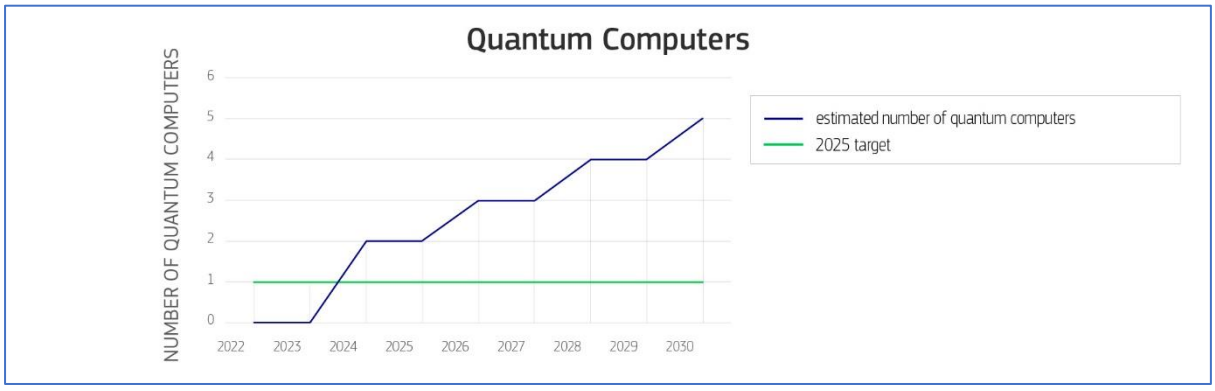
- *increase investments, stimulate secure and sustainable domestic chip design and manufacturing capabilities and continue their commitment in supporting both essential semiconductors and cutting-edge chips in leading value chain areas;*
- *enable a conducive investment framework including by developing the workforce with the semiconductor skills needed.*

Quantum and High Performance Computing (HPC)

The EU reached and exceeded the target in 2024 as the **first two quantum simulators were deployed in France and Germany**[25]. Moreover, it is expected that six additional quantum computers will be deployed until the end of 2025 as several procurement procedures are currently ongoing.

In their National Roadmaps, **Member States reported investing EUR 4.1 billion in quantum computing** (1% of the total budget of the National Roadmaps), of which EUR 3.8 billion come from private sources. The 63 measures reported mainly focus on supporting R&D and deploying quantum technologies, with roughly one third of the measures dedicated to each area. In their adjustments, Member States primarily focused on R&D for quantum technologies.

Quantum computing is a priority for the EU's leadership as a foundational technology, with frequent technological breakthroughs, increasing geopolitical focus and regions taking measures to secure their interests in this strategic field. Quantum technologies are poised to revolutionise multiple industries, driving innovation in healthcare, transportation, energy, defence, chemicals, and pharmaceuticals. Following the **Quantum Technology Flagship** in 2018, committing EUR 1 billion over a decade to reinforce Europe's leadership, total funding has grown to EUR 7 billion.



Despite being **a leading source of public funding for R&I in quantum**[26], **the EU still struggle to mobilise private finance to scale up**, attracting only 5% of global private funding (50% goes to US companies)[27]. This limited private funding hinders the scale-up capacity and contributes to brain drain and intellectual property migration. Moreover, it creates dependence on non-EU capital and

[25] Key Performance Indicators for Quantum Technologies in Europe, Strategic Advisory Board of the European Quantum Flagship, March 2025.

[26] The signature of the Quantum Declaration by 26 Member States confirming the strategic importance of quantum technologies and committing to collaborating on the development of a world-class quantum technology ecosystem across Europe.

[27] Draghi, M., The future of European competitiveness, 2024. According to another independent report by Olivier Ezratty, several US quantum firms attracted private VC funding in hundreds of millions of dollars whereas most EU start-ups operate with under EUR 20 million (Opinions Libres, Understanding quantum technologies 2024).

platforms, putting the EU's quantum sovereignty at risk, especially for hardware and full-stack quantum solutions.

The **European Investment Council has already invested over EUR 200 million in all the fields of quantum technologies** (sensing, communication and computing) and announced **a new STEP Scale-Up scheme**[28]**, making up to EUR 900 million of deep tech scale up funding available**.

The Commission is fostering the development of **Quantum Pilot Lines** to strengthen Europe's strategic autonomy in quantum technologies. In 2025, **six pilot lines for quantum chips were selected** under the Chips Joint Undertaking (JU), bridging laboratory prototypes and industrial manufacturing. QU-PILOT ensures technology maturation (TRL 4 – 7), quality control, and certification processes, paving the way for the future stability pilot lines under the Chips JU (TRL 8 – 9). It offers open access to support startups, SMEs, and academia, preventing a critical gap between R&D and industrial production. **The Quantum Strategy and Quantum Act** will set out the EU's plans to establish itself as the global leader in quantum technologies by 2030 and beyond.

The **High-Performance Computing JU** (EuroHPC) is contributing fully to the Digital Decade's quantum acceleration target by 2025 and has already selected **eight sites across the Union to host the first EU quantum computers** in Czechia, Germany, Spain, France, Italy, Poland, Luxembourg and the Netherlands.

Since its establishment in 2018, EuroHPC is leading the development of a world class supercomputing infrastructure. Over the past five years, EuroHPC has contributed to the acquisition of eight supercomputers, including computers that are among the most powerful in the world. These computers include LUMI (ranked #8 globally), Leonardo (#9), and MareNostrum 5 (#11), which collectively multiply Europe's computational capabilities. EuroHPC has also helped develop the first European system to reach the exascale frontier (JUPITER), which will become fully operational in Q2 2025. A second exascale supercomputer (Alice Recoque) is to be installed within the next year. Two further mid-range EuroHPC systems in Greece and Sweden are currently being procured. These efforts have contributed to developing a world-leading, secure, and interconnected supercomputing ecosystem, broadening HPC usage, and cultivating essential skills for European science and industry.

With the launch of the AI Factories initiative, nine new AI optimised supercomputers will be procured and deployed across the EU in 2025 and 2026, to match the EU's ambition of becoming a leading AI Continent. EuroHPC supercomputers have already enabled many scientific breakthroughs. For example, in 2024 the unprecedented and unique kilometre-scale Earth system models and global multi-decadal climate projections up to year 2050 were made possible through cooperation between EuroHPC and the EU's Destination Earth initiative[29]. This initiative has contributed to better predicting and mitigating the effects of climate change and extreme weather events in the EU.

Both HPC and quantum computing will play a key role in the development of AI Factories and Gigafactories as presented in the AI Continent Action Plan. The AI Factories will deploy and operate AI-dedicated supercomputers connected to large data centres. These Factories will support AI startups and research ecosystems by providing supercomputing services for the large-scale training and development of trustworthy and ethical AI models, particularly in health, climate change, robotics, and automated driving. Additionally, AI Factories will foster talent development through advanced education, training, and reskilling programmes for AI stakeholders.

[28] European Innovation Council, STEP scale up.
[29] Available at: https://destination-earth.eu/.

Quantum technologies - Recommended policies, measures and actions

Member States should:

- step up and coordinate investment in quantum technologies across Member States, and strive to increase private sector investment;

- strengthen efforts in the area of AI infrastructure, with robust support to the AI Factories and other EU initiatives in the field of AI, fostering a collaborative environment and maximizing the impact of these efforts.

b. Foster dissemination of digital technologies in the economy

A key factor undermining Europe's competitiveness is the **insufficient dissemination of digital technologies across its economy.** This limited uptake hampers productivity growth and limits businesses' ability to leverage technology for the creation of innovative services and business models[30].

Achieving a **basic level of digital intensity** among more than 90% of EU SMEs is a key target of the **EU's Digital Decade strategy**. As of 2024, 72.9% of SMEs had reached at least a basic level of digital intensity, up from 69.0% in 2022—a modest 2.8% annual growth. This is insufficient to reach the 2030 target before **2045**, with only 67.9% of SMEs expected to meet the target by **2030**.

Progress is uneven across **Member States** and **sectors**. While countries like **Finland** and **Denmark** have already met the target, others remain well below the EU average. Digital intensity also varies significantly between industries, with high-tech sectors like **ICT** outperforming traditional sectors such as **construction**, **accommodation**, and **food services**. SMEs face several barriers to digitalisation, including a limited awareness of digital technologies and cybersecurity, lack of funding for digitalisation, and digital skills shortages. To address these, the EU and Member States have introduced support measures such as **knowledge-building initiatives**, **financial incentives**, and **ecosystem partnerships**. In their **National Roadmaps**, 166 measures corresponding to a total of EUR 48.2 billion were reported as supporting the digitalisation of SMEs. The measures primarily focus on facilitating the uptake and deployment of digital technologies, as well as strengthening the broader ecosystem through activities such as information sharing, knowledge exchange and collaboration on digital technologies.

A cornerstone of this support is the **European Digital Innovation Hubs (EDIHs)** network, launched in 2023, now covering nearly 90% of the EU's regions. EDIHs provide training, networking, funding advice, and opportunities for SMEs to test digital solutions before investing[31]. Thousands of **digital maturity assessments** have helped SMEs identify areas for improvement, with 90% of participants showing increased digital maturity after engaging with EDIHs. The **Digital Maturity Assessment Tool (DMAT)** shows that SMEs average a score of 40/100, which indicates a moderate level of digitalisation, with relatively strong areas like **data management and cybersecurity**, while **AI & automation** remains weak. Progress in advanced digital areas often depends on solid foundations in strategy, employee engagement, and data handling. Sectors like **finance** and **ICT** lead in digital maturity, while **agriculture**

[30] Europe's choice, Political Guidelines for the next European Commission 2024–2029, 2024 (page 9).

[31] De Nigris, S., Kalpaka, A. and Nepelski, D., *Characteristics and regional coverage of the European Digital Innovation Hubs network, Publications Office of the European Union*, Luxembourg, 2023, doi:10.2760/590526, JRC134620.

and forestry lag behind. On average, firms working with EDIHs improve their DMAT scores by **seven points** in the second assessment, reflecting the effectiveness of targeted support in advancing SME digital transformation across the EU[32].

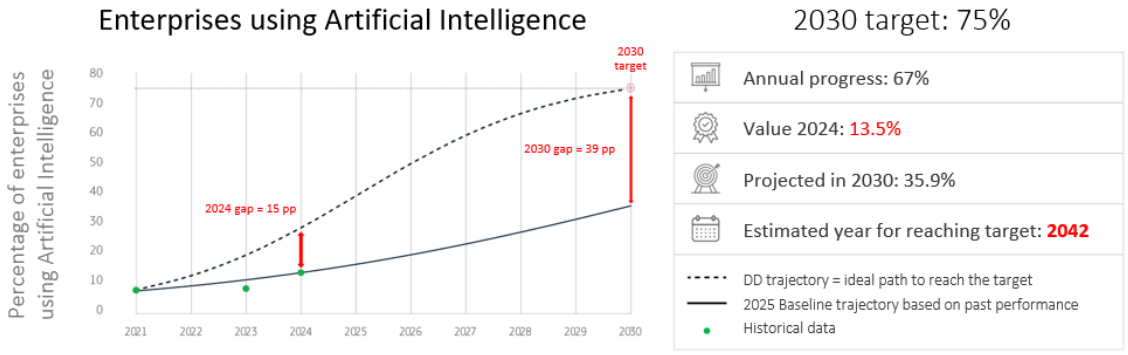
Digitalisation of SMEs - Recommended policies, measures and actions

Member States should strengthen their policies to accelerate SME digitalisation, with a particular focus on the integrating and adopting AI and tailored support within the framework of EDIHs and testing and experimentation facilities (TEFs).

i. Take up of AI

AI has become a critical factor for competitiveness across all sectors of the economy. In 2024 the share of EU enterprises using **AI rose significantly from 8.1% to 13.5%—a 67%** year-on-year increase. However, this remains well below the Digital Decade target of 75% by 2030, which **is not expected to be met until 2042**, with only 35.9% adoption projected by 2030.

Large enterprises continue to lead in AI adoption, with a usage rate of 41.2%, compared to 12.6% among SMEs—a gap of nearly 29 percentage points. However, an encouraging trend is that small companies are accelerating, showing a 71% growth rate, more than double that of larger firms.



AI uptake is advanced in a few sectors - information and communication, and professional, scientific, and technical service, whereas the construction and accommodation are well below the average. Adoption rates vary across the EU, ranging from 27.6% in Denmark to 3.1% in Romania. Nevertheless, growth is broadly distributed, with the fastest increases often seen in countries that previously had low uptake.

In their **National Roadmaps,** Member States reported investments of EUR 10.9 billion to support the uptake of AI, cloud or data analytics – representing approximately 4% of the total budget across roadmaps and covering 196 measures in total. Among these, roughly 34 measures specifically target AI, accounting for EUR 1.3 billion. The measures supporting the uptake of AI, cloud and data analytics are evenly distributed across measures to enhance the ecosystems and knowledge exchange, establish enabling framework conditions and develop capabilities across these technologies. However,

[32] European Commission: Joint Research Centre, Carpentier, E., D'Adda, D., Nepelski, D. and Stake, J., *European Digital Innovation Hubs Network's activities and customers*, Publications Office of the European Union, Luxembourg, 2025, https://data.europa.eu/doi/10.2760/7784020, JRC140547; and Joint Research Centre, Nepelski, D. and Stake, J., *The EDIH SME DMAT 2.0: Revision of the EDIH Digital Maturity Assessment Framework for SMEs*, Publications Office of the European Union, Luxembourg, 2024, JRC141446.

the AI-specific measures place a stronger emphasis on building AI capabilities. This focus is also reflected in Member States' roadmap adjustments.

Overall, while momentum is building, reaching the EU's AI targets will require more targeted actions and support, especially for SMEs and those sectors and regions lagging behind.

Following a slowdown in 2022 and 2023, AI investments have bounced back strongly. According to Dealroom, global venture capital investments in AI reached USD124.9 billion in 2024, marking a 58 percent increase on 2023[33], while private investments in AI in the EU grew by 22 percent in 2024 to USD 10.8 billion[34].

A **key measure is the GenAI4EU initiative**, which takes a sectoral approach and has so far **allocated close to EUR 700 million in planned Horizon Europe and Digital Europe programme** calls in 2025. GenAI4EU aims to stimulate the uptake of generative AI in a wide range of sectors fostering collaboration between AI startups and deployers of AI in industry and the public sector. GenAI4EU is dedicated to unlocking the revolutionary potential of generative AI through ambitious projects. In particular, the initiative aims to optimise production lines in manufacturing, improve robot autonomy and human-robot collaboration in complex tasks, as well as to increase the EU's cyber-defence and medical imaging capabilities.

At the AI Action Summit in Paris, the Commission announced **InvestAI**, an initiative to mobilise EUR 200 billion for investment in AI. This includes the launch of the InvestAI Facility, with a view to mobilise EUR 20 billion investment in AI infrastructure. The investment will support in particular up to **five AI Gigafactories** across the EU, building on the EUR 10 million invested in supercomputing infrastructures and AI Factories in 2021-2027.

The AI Office has been actively working on boosting AI adoption through various support instruments to boost technological integration across Member States. Recently, the EU has intensified its focus on AI adoption, designating it as a main priority to ensure competitive and innovative growth. The various initiatives mentioned in this chapter are part of the **AI Continent Action Plan** published on 9 April 2025. The plan outlines a set of actions on computing infrastructure, data, the development of AI algorithms and adoption, skills, and regulatory simplification to make the EU a global leader in AI.

Moreover, the Commission is adopting the **Apply AI strategy** to boost new industrial uses of AI and to improve the delivery of a variety of services. The strategy will assess the potential of AI technologies in strategic sectors, including advanced manufacturing; aerospace; security and defence; agri-food; energy and fusion research; environment and climate; mobility and automotive; pharmaceutical; biotechnology; advanced materials design; robotics; electronic communications; cultural and creative industries; and science. Furthermore, the public sector will be a driver of the strategy. To ensure consistency among the different support measures for AI, the Apply AI strategy, on which a wide array of stakeholders and the public are consulted, will strengthen the interplay and effectiveness of support instruments and target them towards the needs of AI adopters.

The Apply AI strategy will identify policy actions and concrete deliverables per sector, with key performance indicators to be achieved. The Commission will contribute to supporting developments through its funding programmes as well as through enablers. These enablers include the AI Factories and Gigafactories, Data Spaces, Testing and Experimentation Facilities, European Digital Innovation

[33] Dealroom, Artificial intelligence, 2024. Available at: https://app.dealroom.co/sector/technology/artificial%20intelligence/overview.
[34] Dealroom, Artificial intelligence, 2024. Available at: https://app.dealroom.co/sector/technology/artificial%20intelligence/overview?hqType=regions&hqValue=EU27.

Hubs, and AI Skills Academies. This, in turn, will support AI uptake by European enterprises and the public sector.

AI Factories are open and dynamic AI ecosystems created around the public network of Europe's world-leading EuroHPC supercomputers. They support the EU AI industrial and research ecosystems by bringing together computer power, data and talent to create cutting-edge, trustworthy AI models and applications. They foster collaboration across Europe, unlocking the potential of AI companies, in particular SMEs and start-ups, universities, and industry. AI Factories serve as one-stop shops driving advancements in AI applications across various sectors, such as health, manufacturing, climate and finance. In December 2024, seven consortia were selected to host the first AI Factories[35], and in March 2025, the EuroHPC announced the selection of another six new AI Factories[36]. These AI Factories are expected to more than triple the current EuroHPC AI computing capacity. Overall investments in supercomputing infrastructures and AI Factories in the EU will reach EUR 10 billion between 2021 and2027.

In parallel, **European Digital Innovation Hubs (EDIHs)** will function as AI Experience Centres providing stakeholders with the opportunity to test AI solutions before investing in them, but also offering funding advice, networking opportunities, and trainings. From December 2025, EDIHs will increasingly focus on AI uptake and ensure the adoption of AI solutions across sectors.

The **Network of European Digital Innovation Hubs** will work in close **synergy with the AI Factories ecosystem**. Among others, it will facilitate companies' access to the computing and data resources of the AI Factories, as well as to other AI initiatives, including regulatory sandboxes and testing and experimentation facilities. Increasing the level of AI skills in the Union is one of the priorities that the Apply AI strategy will pursue, as an AI-literate workforce is necessary to boost AI uptake. In particular, the **AI Skills Academy** will function as a one-stop shop providing education and training on skills for developing and deploying AI, and in particular generative AI. Looking ahead, interested Member States with the support of the Commission are designing a possible new **Important Project of Common European Interest** focused on AI, known as IPCEI-AI. The goal is to support R&D&I and first industrial deployment activities, aiming to develop innovative AI technologies and services, such as capabilities for training and deploying foundational models, such as AI models tailored to specific use cases.

Best practice highlights

The **Best Practice Accelerator's (BPA)**[37] **Technology Take-up Cluster**, launched in August 2024 under Belgium's leadership, supports Member States in scaling up the adoption of advanced digital technologies by promoting high-level, replicable national initiatives. As part of the Digital Decade governance framework, the cluster has so far organised two workshops—focusing on AI uptake and on data and interoperability—with the participation of all Member States and presentations from Belgium, Greece, and Finland. Eight best practices have been submitted by Belgium, Denmark, Finland, Germany, Hungary, and the Netherlands, covering themes such as AI adoption, SME digitalisation, personal data control, supply chain optimisation, IPv6 roll-out, and national tech strategies. Workshops were marked by high Member State engagement and interest in the replicability of the

[35] They were submitted by Finland (with Czechia, Denmark, Estonia, Norway and Poland), Italy (with Austria and Slovenia), Spain (with the participation of Portugal, Romania and Türkiye) as well as Luxembourg, Sweden, Germany, and Greece.
[36] Located in Austria, Bulgaria, France, Germany, Poland, and Slovenia. Bringing together 17 Member States and two EuroHPC Participating States.
[37] The Best Practice Accelerator (BPA) is a platform that enables Member States to share successful measures and challenges encountered in their efforts to meet their Digital Decade targets and objectives. Best practices are available to all Member States via the BPA Repository and showcased in regular workshops, currently focused on three thematic clusters: Digital Skills, Green IT, and the Uptake of Digital Technologies.

practices shared. Upcoming sessions will continue to explore enabling frameworks and support schemes to accelerate the widespread use of frontier technologies.

Take up of Cloud-AI-Big Data - Recommended policies, measures and actions

Member States should:

- *take targeted measures and earmark resources to support the adoption of advanced, trustworthy and sovereign AI-enabled solutions; step up investment, also by mobilising the private sector, in general purpose/generative AI.*
- *focus national efforts on incentivising infrastructure investments to ensure that businesses and the public sector have access to the compute infrastructure required for serving their cloud and AI needs, especially for fine-tuning and inference operations.*
- *foster secure and trusted data sharing, supporting the deployment of European Data Spaces, including via practical tools such as model contract clauses, taking full advantage of relevant existing EDICs and accelerating those being prepared.*

c. Security & harnessing digital for EU's resilience in a context of hybrid threats

i. Cybersecurity

The Cybersecurity landscape

As geopolitical and economic tensions grow, cyber threats escalate with espionage, sabotage, and disinformation campaigns becoming key tools for nations to manipulate events and secure a strategic advantage. Cyberespionage campaigns targeting EU Member States and EU institutions, bodies and agencies are continuous and remain a persistent and severe threat. In the context of the cybercrime ecosystem, ransomware remains one of the most impactful threats for EU Member States. There has been a shift from encryption to data exfiltration and with SMEs becoming a more attractive target for cybercriminals, and the double extortion tactic has become the norm for well-established ransomware groups[38]. In 2024, the healthcare sector was particularly affected, with ransomware accounting for 71% of cyber incidents impacting patient care[39]. Meanwhile, ransomware attacks rose by 11% compared to 2023, but enforcement actions against major groups like LockBit have led to a more fragmented threat environment, with 46 new ransomware groups identified in 2024[40].

Supply chain attacks have also surged. Cybercriminals exploit weaknesses in third-party vendors and service providers. This is particularly problematic where there is reliance on technology from high-risk suppliers subject to the jurisdiction of a third country that requires reporting information on software or hardware vulnerabilities to its authorities before they know to be exploited. States-sponsored actors may also preposition themselves in critical infrastructure with the intention of causing disruption later, for example during a conflict. Internet of Things malware attacks increased by 107% in the first half of 2024[41]. There have been concerning trends in public cybersecurity awareness[42] ,with declining confidence among the EU population in their ability to protect themselves from cybercrime and generally low awareness about reporting mechanisms. Overreliance on a single vendor for critical

[38] ENISA, 2024 Report on the State of Cybersecurity in the Union, 2024.

[39] Joint Research Centre, Cyber security in the health and medicine sector, 2024.

[40] Cyberint platform, Ransomware Annual Report 2024, 2025.

[41] SonicWal, SonicWall 2024 Mid-Year Cyber Threat Report, 2024.

[42] ENISA, 2024 Report on the State of Cybersecurity in the Union, 2024.

operations, especially non-European vendors, can result in major risks to all sectors of the economy, as evidenced by recent major incidents like the CrowdStrike outage of 2024.

With an estimated 299 000 cybersecurity professionals missing in its workforce, the EU faces a critical gap[43]. The Cybersecurity Skills Academy[44] contributes to addressing this challenge with concrete actions entrusted to the EU Agency for Cybersecurity (ENISA), such as developing the European Cybersecurity Skills Framework (ECSF)[45] or piloting a cybersecurity skills attestation scheme supporting recognition and portability of skills acquired by cybersecurity professionals.

Cybersecurity in enterprises

When it comes to cybersecurity in enterprises, 92.8% of surveyed enterprises[46] with more than 10 employees in the EU used at least one ICT security measure in 2024. Only 35.5% of the enterprises had documentation on measures, practices or procedures on ICT security, and only 34.1% of them had carried out an ICT risk assessment. Commonly used measures included strong password authentication (83.7% of enterprises) and data backups in a separate location (79.2% of enterprises). According to Eurostat, in 2024, 21.5% of enterprises experienced ICT-related security incidents leading to some adverse consequences.

The median information security spending rose to 9.0% of IT budgets (up 1.9 percentage points)[47], with higher perceived maturity in entities already covered by the Network and Information Security (NIS) Directive[48]. Among all sectors, the telecommunications sector ranks highest in maturity[49].

Despite their critical role in cybersecurity and digital resilience, the deployment of key Internet standards in the EU remains slow and fragmented. IPv6 adoption in the EU stands at **36.4% (user-side)** and **16.8% (server-side)**, with significant disparities across Member States: adoption in some exceeds 40% (e.g. Belgium, France, Germany), while it remains below 10% in others (e.g. Croatia, Cyprus, Malta)[50].

In their **National Roadmaps**, **Member States reported 38 measures contributing to increased cybersecurity**. Almost half of these measures are dedicated exclusively to cybersecurity, with a total budget of EUR 0.8 billion. The other measures have a broader scope, aiming to support several targets across all areas, with a total budget of EUR 6 billion. These initiatives often involve developing national cybersecurity strategies, establishing cybersecurity centres, boosting cybersecurity skills and strengthening cybersecurity capacities in businesses, public services and digital infrastructure. This focus is also reflected in the Member States' roadmap adjustments.

In the period 2024 - 2025, the EU significantly advanced its cybersecurity agenda. The **NIS2 Directive,** which had to be transposed into national law by October 2024, sets a high level of cybersecurity for entities operating in **18 critical sectors**. Moreover, in October 2024, the Commission adopted the first implementing act under the NIS2 Directive, specifying the cybersecurity risk management measures and the cases in which an incident should be considered significant for companies providing digital

[43] ISC2, 2024 Cybersecurity Workforce Survey Focus on the E.U, 2024.
[44] Please see the website: https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy.
[45] European Cybersecurity Skills Framework (ECSF) | ENISA.
[46] Eurostat (isoc_cisce_ra) and (isoc_cisce_ic); Eurostat, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprisesICT security in enterprises, 2024.
[47] Compared to 2022. ENISA, NIS Investments 2024, 2024.
[48] Directive (EU) 2016/1148 repealed by Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive).
[49] ENISA, 2024 State of Cybersecurity Report, 2024.
[50] EU Internet Standards Deployment Monitoring Website, available at: https://ec.europa.eu/internet-standards/downloads.html.

infrastructures and services. The **Cyber Resilience Act**[51], in force since December 2024, mandates cybersecurity requirements for digital products, with full implementation within three years. The **Cyber Solidarity Act**[52], effective since February 2025, established a European Cybersecurity Alert System, consisting of Cyber Hubs that would use advanced technologies and AI-driven threat detection. The act also laid the groundwork for the Cybersecurity Emergency Mechanism and the Incident Review Mechanism. The **Cybersecurity Act**[53]was effectively amended in February 2025 to enable the possible certification of managed security services. A **European action plan on the cybersecurity of hospitals and healthcare providers**[54] was adopted in January 2025, improving sectoral preparedness. Finally, in February 2025, the Commission proposed a revised **Cybersecurity Blueprint**, integrating civil-military coordination and crisis response mechanisms[55].

Work is also progressing on the European Quantum Communication Infrastructure (EuroQCI), which is part of the Union Secure Connectivity Programme (IRIS²). EuroQCI will provide, in first instance, a highly secure, quantum-protected service for the exchange of cryptographic keys, for symmetric encryption of communications between governmental entities and for protecting critical infrastructures. Throughout 2024, efforts focused on deploying national quantum communication networks, advancing key European technologies, and preparing for the deployment of quantum communication in space. Deployment of cross-border connections will start in 2026. The current EuroQCI efforts on point-to-point links and more complex networks are initiating the long-term endeavour of transitioning to future networks fully based on quantum technologies. However, the threat posed by quantum computing to cryptography must be addressed now, in a manner that is compatible with the way modern digital networks are designed and function. The transition to **Post-Quantum Cryptography (PQC)** remains essential, and such technology will likely play a highly relevant role also to support or hybridize with future quantum networks. To guide this transition, the Commission published a Recommendation in 2024 encouraging the Member States to develop a Roadmap to ensure a synchronized transition to PQC for public administrations and critical infrastructures across the EU. Work on developing this roadmap is ongoing, in the context of the PQC workstream in the NIS Cooperation Group, and it is also accompanied and supported by the sectorial developments, deployments and mapping of activities in several EU projects and other Member States' initiatives.

Cybersecurity - Recommended policies, measures and actions

Member States that have not already done so shall transpose the NIS2 Directive as a matter of urgency and should take actions, also going beyond what is necessary, to maximise the effects of the full implementation of the cybersecurity acquis, including the NIS2 Directive and the 5G cybersecurity Toolbox (encompassing where appropriate the imposition of restrictions or exclusions as regards high-risk suppliers).

Moreover, Member States should:

[51] Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).
[52] Regulation (EU) 2025/38 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act).
[53] For more information, please see the website: https://digital-strategy.ec.europa.eu/en/library/proposed-regulation-managed-security-services-amendment.
[54] European action plan on the cybersecurity of hospitals and healthcare providers, COM (2025) 10 final.
[55] For more information, please see the website: https://digital-strategy.ec.europa.eu/en/news/commission-launches-new-cybersecurity-blueprint-enhance-eu-cyber-crisis-coordination.

- *step up efforts to increase cybersecurity capabilities, including relevant to ensure the development of skills for the cybersecurity workforce by making use of available resources at EU level such as the European Cybersecurity Skills Framework;*
- *within the NIS Cooperation Group, develop a roadmap to ensure a synchronized transition to PQC throughout the whole EU for public administrations and critical infrastructure;*
- *progress in the transition of their crypto systems to post quantum cryptography by 2035, ensuring intermediate milestones are also met for high risk use cases and/or very complex systems to be migrated by 2030.*

ii. Submarine cables security

In February, the EU adopted the **Action Plan on Cable Security** to strengthen the resilience of its submarine cable infrastructure, including data cables, following a full resilience cycle—**prevention, detection, response, recovery, and deterrence**. The Commission, alongside the High Representative, will engage with Member States and partners, including NATO, to operationalise a number of concrete actions.

To prevent incidents that could compromise the EU's security and resilience, the Action Plan sets out dedicated actions to improve the redundancy and security of telecommunications cables. A key component of this effort is the allocation of nearly EUR 1 billion from the CEF Digital programme to strengthen backbone connectivity, with a focus on cross-border digital infrastructure and to connect EU territories with likeminded third countries. The Action Plan also promotes strengthening security requirements, in accordance to both the NIS2 and CER Directives. As set out in the prevention section of the Action Plan, an Expert Group comprising Member State representatives and ENISA has been established to deliver on Recommendation (EU) 2024/779 on Secure and Resilient Submarine Cable Infrastructures[56]. The Action Plan specifies that by Q4 2025, the Expert Group is expected to complete key tasks, including a comprehensive mapping of existing and planned infrastructures, a coordinated risk assessment (including the development of a stress testing methodology), the creation of a Cable Security Toolbox of mitigating measures, and a priority list of Cable Projects of European Interest (CPEIs) to be co-funded by CEF Digital. To increase the capacity to detect potential threats and incidents early on, the **Action Plan further proposes to establish an integrated surveillance mechanism.** This mechanism will be facilitated through the voluntary set up of regional cable hubs, located in each sea basin, which will serve as centres for monitoring and analysing the status of submarine cables, including potential suspicious activity occurring nearby. Additionally, the Action Plan provides for investments in new technologies, such as smart cables, undersea sensors and drones, to improve detection capacities.

The Action Plan sets out a more efficient response to incidents, building synergies between existing EU crisis management frameworks such as the EU Cyber Blueprint and the Critical Infrastructure Blueprint. To reduce the time to repair and mitigate the impact of incidents, it also calls for **increased repair capacities**. To that end, the Commission has proposed to support modular equipment that can be plugged to civilian vessels, and the gradual establishment of an EU Cable Repair Fleet.

To strengthen the security and resilience of submarine cables, a central role will be played by the CEF Digital programme, including for: i) providing direct support to the funding of strategic cables (over 420 million already committed in the first three calls); ii) enhance our ability to monitor and trigger

[56] Commission Recommendation (EU) 2024/779 of 26 February 2024 on Secure and Resilient Submarine Cable Infrastructures, *OJ L, 2024/779, 8.3.2024.*

early response actions in case of suspicious events (early warning systems); iii) support the deployment of functional modules for the repair and deployment of cables.

Finally, to **deter malicious actors from engaging in harmful activities,** the Action Plan calls for a significant strengthening of efforts to counter the shadow fleet of vessels. It also emphasises the importance of boosting cable diplomacy and promoting a common interpretation of international maritime law.

Submarine cable security: Recommended policies, measures and actions

Member States, together with the Commission, should:

- urgently operationalise the different actions outlined in the Action Plan. Building on the transposition of NIS 2 and CER, priority should be given to the aim of ensuring comprehensive cable security.

- fast-track key deliverables, including the Expert Group's tasks (mapping, risk assessments, Cable Security Toolbox, priority Cable Projects of European Interest), the development of a common strategy to reinforce cable repair capacities, and the establishment of Regional Cable Hubs. The goal of these hubs will be to establish an integrated surveillance mechanism for the EU to monitor and respond to cable security threats, in coordination with the cable repair capacities.

3. Protecting and empowering people, preserving EU democracies and values

a. Empower people through digital skills

Empowering citizens and equipping workers with digital skills are at the core of Europe's digital transformation, in line with the Declaration on Digital Rights and Principles. Basic digital skills are essential for economic participation, social inclusion, and democratic resilience, while the availability of highly skilled professionals—particularly ICT specialists—is critical to Europe's competitiveness, technological sovereignty, and strategic autonomy.

Despite growing awareness of the need to boost digital skills across society**, the pace of progress in this area remains insufficient.** In 2023, only 55.6% of adults had at least basic digital skills[57]. On the basis of current trends, the EU is expected to reach a level of just under 60% by 2030 – falling significantly short of the 80% target set in the context of the Digital Decade policy programme[58]. This shortfall is particularly evident among certain demographic groups. For example: older adults, people with low levels of education, and people not in work or looking for work face disproportionately high risks of digital exclusion[59]. Although young people are often seen as digitally 'native', they are not universally digitally literate: 43% of eighth-grade students (aged 13 to 14) do not reach basic levels of digital skills, with persistent disparities based on socio-economic background and geographical location[60].

[57] Eurostat, European Union Survey on the Use of ICT in Households by Individuals. Available at: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators

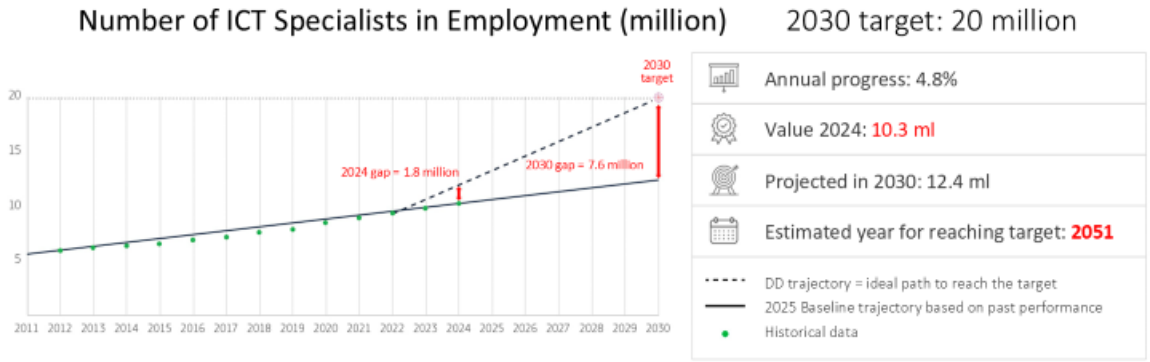
[58] At least basic digital skills in the EU. Historical data, Digital Decade trajectory and revised baseline trajectory towards 2030.

[59] European Commission, Joint Research Centre, Bertoni, E., Cosgrove, J., & Cachia, R. (2025). Digital Skills Gaps – A Closer Look at the Digital Skills Index (DSI 2.0), 2025. JRC140617.

[60] ICILS 2023 International Report: An International Perspective on Digital Literacy. Available here: https://www.iea.nl/studies/iea/icils/2023

At the same time, the **need for ICT specialists is rising sharply.** As the architects of Europe's digital future, these professionals play a central role in deploying advanced technologies, increasing productivity, and delivering secure and efficient digital services. Nevertheless, the EU remains only **halfway toward reaching its 2030 target of having 20 million ICT specialists in employment.** Structural shortages persist, hindering growth in high-demand digital areas such as AI, cybersecurity, and semiconductors. In 2024, women accounted for 19.5% of employed ICT specialists, a figure virtually unchanged from 19.4% in 2023.

To address these challenges, the Commission, in partnership with Member States, has put in place a comprehensive framework to strengthen digital skills across society. The **Skills package**[61], adopted in March 2025, puts a strong focus on digital skills as a key driver for competitiveness. It includes the **Union of Skills**, an **Action Plan on Basic Skills**[62], a **STEM Education Strategic Plan**[63], and the upcoming **2030 Roadmap on the future of digital education and skills**. To strengthen **leadership in key digital technologies**, the Commission is prioritising the development of advanced digital skills, ICT talent attraction and a resilient, future ready digital workforce. This also includes initiatives such as the recently adopted **AI Continent Action Plan** and the upcoming **Apply AI strategy**.



To respond to the need for a more coordinated approach to digital skills education and training in the EU, targeted at emerging skills needs of European companies, the European Commission is funding and promoting three new **Digital Skills Academies in Quantum, AI, and Virtual Worlds**. These academies will leverage strategic partnerships and act as powerful catalysts for promoting digital careers. The **Cybersecurity Skills Academy,** which already helps Member States to scale up training provision and improve coordination between industry and education providers, is being further expanded. Furthermore, through the **Chips Act** and the establishment of **Chips Competence Centres**, the Commission and Member States are investing in national talent pipelines for the semiconductor sector, supporting advanced technical training and collaboration with industry.

In their **National Roadmaps,** Member States reported investments of EUR 24.6 billion in basic digital skills (9% of the total budget). The 339 measures reported on the roadmaps primarily focus on improving digital skills in formal education and promoting digital inclusion, with roughly one third of the measures dedicated to each area. This emphasis on building digital skills is also evident in Member States' roadmap adjustments. For training of ICT specialists, Member States reported investing EUR 11.8 billion (4% of the total budget). The 213 measures on ICT Specialists mainly focus on increasing the number of people with advanced and highly specialised digital skills, with around one third of these measures targeting individuals in formal education and approximately one quarter of the measures focusing on those already in employment. This focus is also reflected in the Member States'

[61] European Commission, A Union of Skills to Equip People for a Competitive Europe, Press Release, Brussels, 5 March 2025.
[62] European Commission, Action Plan on Basic Skills, 2025.
[63] European Commission, STEM Education Action Plan, 2005.

roadmap adjustments, which include a sharp increase in measures aimed at boosting advanced digital skills among women.

National efforts have been strengthened through collaborative mechanisms. The 2024 edition of the **European Digital Skills Awards**[64] recognised outstanding projects promoting inclusion, digital literacy, and bridging digital divides. At the same time, the **Digital skills and Jobs Platform**[65] continues to grow as a central hub–for accessing learning opportunities, connecting over 15 000 stakeholders across Europe.

However, as laid out in the Draghi report and reiterated in the **Competitiveness Compass**, Europe is facing massive investment needs **for education and skills development in sectors critical to European competitiveness and preparedness.** Mobilising public and private investments, pursuing growth-enhancing reforms, and leveraging multi-country projects will be key to closing the talent gap in digital skills.

The European Commission is supporting the development of the Common European **Data Space for Skills** to improve our knowledge of what skills are likely to soon be in demand, helping policymakers and educators to anticipate future needs and direct investments more effectively. Furthermore, given the mounting **global competition for digital talent**, the EU is stepping up its support to Member States and employers to attract highly skilled top-tier researchers and professionals by establishing Multipurpose Legal Gateway Offices in selected partner countries. Where relevant, these could underpin Talent Partnerships as well as the future EU Talent Pool. In addition, the EU will also act to support portability of skills, addressing barriers to workers' mobility.

Best practice highlights

The **BPA Digital Skills Cluster**, led by Slovenia, involved all Member States in a structured peer exchange, with best practices submitted by Austria, Belgium, Croatia, Czechia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, Romania, Slovenia, and Spain. While only some submitted practices, all Member States participated in the associated workshops that were held and expressed interest in adapting successful approaches. Of the 34 practices shared, over half focus on boosting basic digital skills for underserved groups, while 15 target the education of ICT specialists through measures such as curriculum reform, AI training, SME upskilling, and gender equality. Five workshops have been held so far, covering topics such as inclusion, education, AI-readiness, and the participation of elderly, rural populations, and women in advanced skills. Future sessions will continue to support inclusion while expanding into ICT specialisation areas such as cybersecurity, semiconductors, and mid-career reskilling.

Digital Skills - Recommended policies, measures and actions

Member States should:

- *Prioritise investment in digital education and skills in line with the Council Recommendation on improving the provision of digital skills and competences in education and training, including targeted policies for groups most in need;*
- *Promote AI literacy and basic cybersecurity practices.*

[64] European Commission, European Digital Skills Awards. Available at: https://digital-skills-jobs.europa.eu/en/european-digital-skills-awards-2025.
[65] European Commission, Digital Skills and Jobs Platform. Available at: https://digital-skills-jobs.europa.eu/en.

ICT specialists - Recommended policies, measures and actions

Member States should:

- *Promote ICT careers among young people, with notably a dedicated attention to girls;*
- *Enhance the academic offer for advanced digital skills and strengthen VET and lifelong learning in order to contribute to the EU's strategic digital objectives in key areas such as AI Factories, cybersecurity, data and semiconductors;*
- *Support the implementation of EU Digital Skills Academies;*
- *Leverage EU funding opportunities and governance structures such as European Digital Infrastructure Consortia (EDICs), the Digital Decade Best Practice Accelerator, and National Digital Skills and Jobs Coalitions;*
- *Increase efforts to expand labour migration pathways to attract highly skilled ICT specialists from non-EU countries and incentivise the return of European ICT talent to the EU, leveraging both national and European frameworks.*

b. Deploy digital solutions for people and societies

User-friendly and accessible digital public services to foster competitiveness and inclusion

In 2024, the EU made steady progress toward its Digital Decade targets for fully digital public services. The citizen score rose to 82.3/100 (+3.6%), and the business score to 86.2/100 (+0.9%). In their **National Roadmaps**, Member States reported investing EUR 13.8 billion, representing approximately 4.8% of the total budget, to drive the digitalisation of key public services. This investment included a comprehensive set of 287 measures, of which more than half aim to increase the uptake, interoperability and accessibility of digital public services and around one-quarter focus on strengthening their security and resilience of these services.

As Member States expand their offering of digital public services, **ensuring technological sovereignty and reducing reliance on foreign technologies** has become an important mean to safeguard privacy, increase resilience, and strengthen trust in EU-governed digital ecosystems. Despite the growing digitalisation of public services across the EU, a very significant share of government digital infrastructure still relies on **non-EU-based service providers** -particularly in areas such as cloud computing, data hosting, software platforms, videoconferencing and cybersecurity solutions. With 80% of the services bought by governments and the private sector originating mostly from the US[66], a substantial share of the **EUR 2 trillion that public authorities spend annually on the purchase of services, works and supplies**[67] **is not being spent on services originating in the EU**. This dependency might pose strategic risks, including reduced control over sensitive data, potential misalignment with EU values and regulatory frameworks, and vulnerability to the application of third country laws. Strategic public procurement, notably thanks to the revision of the Public Procurement Directives, as well as the support to GovTech will play a key role to foster EU preference through public investment and procure innovative solutions, which streamline administrative processes, foster transparency and improve data-driven decision-making.

[66] Draghi, M., The future of European competitiveness, 2024, Part A – A competitiveness strategy for Europe.
[67] European Commission, The Public Procurement Data Space (PPDS). Available at: https://single-market-economy.ec.europa.eu/single-market/public-procurement/digital-procurement/public-procurement-data-space-ppds_en

It is also of the utmost importance to ensure that there is adequate human support to help members of the public navigate digital services, with 9 out of 10 Europeans emphasising the significance of this support in the Digital Decade Eurobarometer survey[68].

In 2024, the use of **AI in public services** expanded further on EU Member States - from decision support and personalised services, to predictive tools in healthcare. A cornerstone of the efforts to reduce administrative burdens and support European Businesses interacting digitally will be the **European Business Wallet** which will streamline business-to-business and business-to-government interactions, enabling secure data exchange while creating new opportunities for trust service providers.

The **Single Digital Gateway** and the **Your Europe**[69] portal are key elements of the EU's digital infrastructure for cross-border public services. Your Europe is the main access point for national procedures and information about rules and rights and is currently the most visited EU website. The **Once-Only Technical System**[70] enables the secure cross-border exchange of evidence. Its common services are operational, and Member States are currently connecting competent authorities to it. A cornerstone of the efforts to reduce administrative burdens and support European Businesses interacting digitally will be the European Business Wallet which will streamline business-to-business and business-to-government interactions, enabling secure data exchange while creating new opportunities for trust service providers. Together with the upcoming **EU Digital Identity Wallet**[71]**, the Single Digital Gateway and the Once-Only Technical System** form an integrated infrastructure for accessing public services across the EU[72]. In addition, the **Public Procurement Data Space** simplifies processes and improves monitoring across the Single Market[73].

Other tools include the Business Registers Interconnection System (BRIS), a key transparency and secure data exchange tool, providing the public with company information and enabling the implementation of the 'once-only' principle with regard to company data and the European e-Justice Portal which are of key importance for the digitalisation of public services and of cross-border judicial proceedings.

The **Interoperable Europe Act**[74], effective from April 2024, marked a significant step towards strengthening interoperability in the public sector and the delivery of digital public services, providing a structural framework to drive seamless, cross-border digital public services within the EU. It introduces interoperability assessments to be carried out by publica administrations to ensure cross-border interoperability (mandatory since January 2025) and regulatory sandboxes. It also embeds

[68] Special Eurobarometer 566 on 'the Digital Decade' 2025, available at this link: https://digital-strategy.ec.europa.eu/en/news-redirect/883227.
[69] European Commission, The Single Digital Gateway and Your Europe. Available at: https://single-market-economy.ec.europa.eu/single-market/single-digital-gateway_en
[70] The Once-Only Technical System (OOTS) streamlines data retrieval for cross-border procedures, enhancing trust, efficiency, and data exchange among EU public administrations and citizens. It is an EC solution. Available at: https://interoperable-europe.ec.europa.eu/collection/digital-building-blocks/solution/once-only-technical-system-oots
[71] Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. See also: European Commission, A Digital ID and Personal Digital Wallet for EU Citizens, Residents and Business. Available at: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home.
[72] European Commission, The Public Procurement Data Space (PPDS). Available at: https://single-market-economy.ec.europa.eu/single-market/public-procurement/digital-procurement/public-procurement-data-space-ppds_en
[73] On these topics and the potential for simplification, please see also section 5.a.i of this document.
[74] Interoperable Europe Act, COM(2022) 720 final.

digital-ready policymaking - ensuring that future EU legislation supports digital transformation from the outset.

Digital public services - Recommended policies, measures and actions

Member States should focus investments and regulatory measures to develop and make available secure, sovereign and interoperable digital solutions for online public and government services, including possibly in the context of public procurements and including the completion of the connection of authorities to the Once-Only Technical System.

i. EU Digital Identity Wallets and European Business Wallets

The **European Digital Identity (EUDI) Framework** is a cornerstone of Europe's digital transformation and a key enabler of Digital Decade targets. Coverage continues to expand with **24 Member States** having now notified their electronic ID schemes, and **95% of EU citizens** now having access to eID. However, Hungary, Greece, and Ireland have yet to notify their schemes.

Central to this EUDI framework are the **EUDI Wallets**, designed to offer every EU citizen and business secure and seamless access to both public and private services across the EU by the end of 2026. These wallets will transform how people interact online - enabling cross-border authentication, legally valid e-signatures, and the digital storage, presentation and verification of key documents such as IDs, educational credentials, ePrescriptions, social security attestations, and driving licences. By replacing multiple logins with a single trusted solution, they increase convenience, privacy, and security for everyday transactions, travel, and access to services.

Moreover, significant legal milestones were reached. The **EUDI Regulation** entered into force in May 2024, followed by the adoption of nine **implementing acts** in November 2024 and April 2025, setting uniform technical standards and putting in place a robust certification framework. These ensure that all wallets are **interoperable, secure**, and **privacy-preserving** across the EU. Member States are now mandated to provide at least one wallet by the end of 2026.

Deployment is being tested through **Large Scale Pilot (LSP) projects**, covering real-world use cases from **education, social security and travel** to **payments and eGovernment services**. Since 2023, four LSPs have been running, involving over **350 entities** from nearly all Member States. In 2025, two new consortia - **WE BUILD** and **APTITUDE** - will further scale this work with over EUR 40 million in EU and Member State funding. These projects cover 17 use cases, including supply chains, business services, vehicle registration certificates, and digital travel credentials. These pilots are supported by the **Digital Europe Programme**.

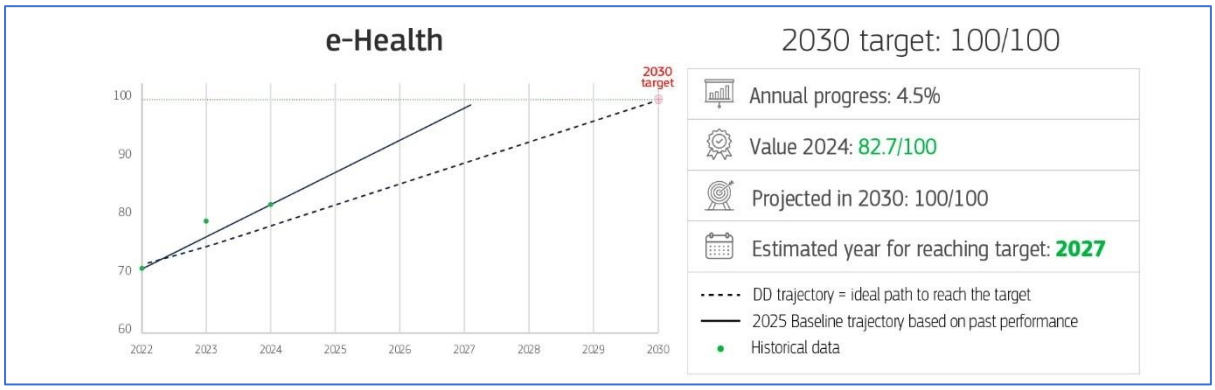
Looking ahead, the **European Business Wallet proposal will build on the EUDI Framework**, is planned in **Q4 2025**. This proposal will seek to facilitate business interactions with public authorities, reduce reporting burdens, and enable secure regulatory compliance across borders. This will in turn increase Europe's competitiveness.

EU Digital Identity Wallets - Recommended policies, measures and actions

Member States should continue their strong commitments to the development of use cases to link private and public service providers to the wallets and offer the user a large variety of use-cases upon first issuance of the wallets at national level in 2026.

ii. eHealth and technologies for healthcare.

In 2024, the EU continued to advance toward its Digital Decade goal of universal access to electronic health records (EHRs) by 2030. The composite score in the area rose to 82.7/100 (from 79.1/100 in 2024), with **all Member States offering some form of EHR access**. Estonia joined Belgium in reaching full coverage, while countries like Czechia, Ireland, Romania, and Slovakia made strong progress. Despite these gains, disparities persist: Austria, Cyprus, and the Netherlands recorded setbacks due to reduced functionalities or service availability. Ensuring the online availability of health records will now also be required under the **European Health Data Space**[75], which entered into force in **March 2025** as part of the EU's efforts to foster the digital transformation of healthcare. The European Health Data Space will increase citizens' control over their personal electronic health data and enable data reuse for research, innovation and policy purposes.



Innovation in medical technologies and life sciences is increasingly being powered by digital health data. Of the 13 first-selected **AI Factories**, 11 will put health and/or life sciences among their focus areas. The **European Cancer Imaging**, **1+ Million Genomes**, and **Virtual Human Twins initiatives** are making progress on setting up data infrastructures to foster personalised care and data-driven research, backed by targeted DIGITAL[76] funding and new procurement instruments. At the same time, the number of healthcare providers contributing data continues to grow, **though private sector participation still lags**. In their **National Roadmaps**, Member States reported investing EUR 7.8 billion to support e-Health services (all coming from public budgets), with approximately 106 measures, most of them focusing on accessibility and uptake. Continued investment, technical alignment, and cross-border cooperation will be essential to fully achieve the **European Health Data Space**. **Cybersecurity remains a key concern**. To strengthen resilience, incident response, and recovery capacities across the sector, the Commission in January 2025 launched a **European action plan on the cybersecurity of hospitals and healthcare providers** - a flagship initiative of the President von der Leyen's 'first 100 days'. Further recommendations to strengthen cybersecurity in the health sector, based on consultations with stakeholders and Member States, will follow in **Q4 2025**.

eHealth - Recommended policies, measures and actions

Member States should:

- *continue to implement the necessary measures to achieve full access for citizens to their electronic health records.*

[75] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847.
[76] European Commission, Digital Europe Programme. Available at: https://digital-strategy.ec.europa.eu/en/activities/digital-programme

- *cooperate to fully deploy the innovation potential of health data by: (i) maximising the use of existing and future health data initiatives and infrastructure; (ii) investing in the research and deployment of advanced technologies such as high-performance computing and trustworthy AI applications in healthcare;(iii) strengthening cybersecurity measures, and enhancing cooperation through EDICs in this area.*
- *Implement the actions foreseen in the Action Plan on cybersecurity of hospitals and healthcare providers.*

iii. Smart cities and the New European Bauhaus: digital for quality of life

To bring **digital innovation closer to citizens and make cities more sustainable** and climate-neutral, the EU has mobilised a range of funding initiatives and multi-country projects, including the DIGITAL programme and newly established EDICs. The **LDT-CitiVERSE-EDIC**, launched in 2024, will help cities harness digital twins and shared infrastructure to address urban challenges—such as **climate neutrality, clean mobility, and smart energy systems**. CitiVERSE aims to bring together **100 cities in 2025** under a common EU digital infrastructure, connected to the first **SIMPL-based Data Space for Smart Communities**. Other projects are also underway to harness digital technologies in societal projects such as the **New European Bauhaus** (NEB)[77] for more sustainable, innovative and beautiful living environment (DigiNEB)[78]. The new **LDT-CitiVERSE-EDIC**[79] will receive within the EU procured LDT toolbox a complete set of digital tools and services to be used together with the EU building dataset for AI-based impact assessment of NEB strategies.

To address the challenge of climate neutrality with a holistic approach, there are also possible synergies with the actions taken under Horizon Europe[80], within the Mission on Climate-Neutral and Smart Cities.

Another initiative funded by the Digital Europe Programme, the **European Data Space for Smart Communities** (DS4SSCC-DEP) is a pivotal deployment project focusing on creating a large-scale data space controlled by public data holders, ensuring alignment with the **Smart Middleware Platform** and broader data space ecosystems. It also aims to offer middleware service solutions facilitating data sharing and management while refining the service it offers based on gained experience.

The Digital Europe Programme also co-finances the testing and experimentation facilities (TEF) for smart cities and communities: CitCom.ai. CitCom.ai provides facilities to test advanced AI and robotics solutions in real-world settings, targeting the sustainable development of cities and communities. CitCom.ai focuses on three overarching themes: (i) **Power** which targets changing energy systems and reductions in energy consumption; (ii) **Move** which targets more efficient and greener transportation linked to logistics and mobility; and (iii) **Connect** which serves citizens through local infrastructures and cross-sector services. CitCom.ai is organised around three super nodes – Nordic, Central and South – supported by satellites and sub-nodes located across 11 EU countries: Denmark, Sweden, Finland, the Netherlands, Belgium, Luxembourg, France, Germany, Spain, Poland and Italy.

The Commission currently manages or contributes to a broad set of initiatives with - and for - cities. The flagship R&I initiative in this field is the Horizon Europe Mission on Climate-Neutral and Smart

[77] European Commission, New European Bauhaus. Availabile at: https://new-european-bauhaus.europa.eu/index_en
[78] DigiNEB. Available at: https://digineb.eu/
[79] European Commission, Citiverse. Available at: https://digital-strategy.ec.europa.eu/en/factpages/citiverse
[80] Specifically, considering the call results of 'HORIZON-MISS-2025-04-CIT-02: Innovative, AI-based solutions for urban planning and management'.

Cities ('the Mission'), which aims to deliver 100 climate-neutral cities by 2030 and ensure that all EU cities follow suit and become climate neutral by 2050[81].

c. Protecting people, including minors, online

i. Preserving safety, security and wellbeing in digital environment

Online platforms have become integral to everyday life in the EU. Services like Google Search, YouTube, and Amazon are used by most Europeans[82] and 77% of internet users shop online[83]. Citizens are also increasingly aware of online risks: in 2023, nearly 70% took action to protect their personal data[84], and 72% reported awareness of the GDPR[85]. However, the sheer volume of user and platform activity - illustrated by over 10 billion content-moderation decisions in the last six months[86] - highlights the urgent need for **robust digital governance**.

The **Digital Services Act (DSA)**, **Digital Markets Act (DMA)** and, among others, the **Terrorist Content Online (TCO) Regulation** are instruments that aim to ensure a fair, safe, secure and trustworthy digital environment for citizens and businesses, accompanied by robust enforcement mechanisms.

The **Digital Services Act (DSA)** indeed represents a landmark EU response to this issue, setting clear obligations for digital service providers and assigning greater responsibilities to Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs). In 2024, the list of services designated as VOLPs grew to 25, including Shein, Temu, and XNXX. To enforce the DSA, the European Commission has sent over 100 Requests for Information (RFIs) to platform providers, targeting disinformation, unsafe products, and opaque advertising practices. In addition, the Commission opened **14 formal proceedings**—for example against the providers of TikTok, Meta, Temu, X and AliExpress—notably focused on illegal content, the protection of minors, and algorithmic transparency. Markedly, one of the proceedings against the provider of TikTok has already been closed after TikTok agreed to binding commitments.

In February 2025 the Commission introduced the **e-Commerce Communication** which sets out a series of cross-cutting measures to ensure that goods sold online for example on digital marketplaces and particularly by non-EU sellers comply with EU rules[87]. By November 2025 the Commission **will evaluate how the DSA interacts with other EU legislation**, in particular legislation on personal data and consumer protection.

ii. Protecting children

As set out in the 2024-2029 Political Guidelines[88], the Commission considers the protection of children's and young people's mental health - particularly online - as one of the greatest challenges of

[81] European Court of Auditors, Special Report: Smart cities Tangible solutions, but fragmentation challenges their wider adoption, 2023.
[82] Digital Services Act (DSA): Amazon EU Store Transparency Report. Available at: https://trustworthyshopping.aboutamazon.com/dsa-digital-services-act-amazon-eu-store-transparency-report; Google Transparency Report: Signed-out recipients, versus 459 million signed-in recipients. Available at: https://transparencyreport.google.com/report-downloads?hl=en; Google Transparency Report: Signed-out recipients, versus 356 million signed-in recipients. Available at: https://transparencyreport.google.com/report-downloads?hl=en; Google, Information about Monthly Active Recipients under the Digital Services Act, 2025.
[83] Eurostat, [isoc_ec_ib20] Internet purchases by individuals (2020 onwards).
[84] At least one of the following: blocked or limited cookies, checked website security where personal data is provided, limited access to social media profile or shared content, read privacy policy statements, refused use of personal data for advertising, restricted or refused access to geographical location. These are the activities used by Eurostat for calculating individuals' safety skills. Indicator: Privacy and protection of personal data (2020 onwards), Eurostat: isoc_cisci_prv20
[85] European Commission, Justice, rights and values, October 2024, Eurobarometer survey
[86] See data of the DSA transparency database: https://transparency.dsa.ec.europa.eu/
[87] European Commission, E-commerce communication: A comprehensive EU toolbox for safe and sustainable e-commerce. Available at: https://digital-strategy.ec.europa.eu/en/library/e-commerce-communication-comprehensive-eu-toolbox-safe-and-sustainable-e-commerce
[88] European Commission, Europe's Choice, Political Guidelines for the next European Commission 2024–2029, 2024.

this decade. The Polish and Danish Presidencies of the EU Council have identified the impact of social media on young people's mental health and the protection of minors online as a priority. In 2024, public concern over the protection of children online continued to rise, with increasing calls across the EU and internationally to address the digital determinants of poor mental health among young people[89]. These calls have largely focused on the regulation of digital technologies and their negative impacts on mental well-being.

According to the 2025 Digital Decade Eurobarometer survey, **an overwhelming majority of respondents believe that urgent action by public authorities is needed** to protect children online, and in particular to: (i) limit the negative impact of social media on mental health (93% of respondents agreed); (ii) restrict access to age-inappropriate content through robust age assurance mechanisms (92% agreed); and (iii) tackle cyberbullying and online harassment (92% agreed)[90]. Increasing screen time has coincided with higher levels of problematic social media use and rising reports of cyberbullying. According to a study by the World Health Organization (WHO), **one in six school-aged children has experienced cyberbullying**[91]. Additionally, **34% of surveyed adolescents reported playing digital games daily**, with 22% playing for at least four hours on a gaming day[92]. Previous research[93] has shown that adolescents with problematic social media use report lower levels of mental and social well-being, as well as higher rates of substance use, compared to non-problematic users and non-users. If this trend continues, it could have far-reaching consequences for adolescent development and long-term health outcomes.

The risks children face online are increasingly severe. In 2024 the **EU co-funded Safer Internet Centres** (SICs) handled over 54 000 calls, 14% of which related to cyberbullying and 24% to sexual content, including grooming and sextortion[94]. In Poland, during the fourth quarter of 2024, every second underage internet user was exposed to erotic content, spending an average of 10 to 14 minutes per day on such material[95].

Excessive screen time, exposure to violent, pornographic or explicit content, and commercial manipulation - often in environments designed for adults - have become frequent experiences for minors, posing significant risks to their mental health. So far, **age-gating tools** that restrict access to content based on age **remain largely ineffective**. Research suggests that intensive use of online social networks is associated with loneliness and emotional distress among young people, a pattern not generally observed with instant messaging tools[96].

The EU has strengthened its legal framework and policy action to protect children online. At the core of the EU toolbox on protection and empowerment of minors online are: the **Digital Services Act**, the

[89] See e.g. Council Conclusions on the European and international policy agendas on children, youth and children's rights, 18 May 2024, https://data.consilium.europa.eu/doc/document/ST-9769-2024-INIT/en/pdf and the follow-up to the WHO-UNICEF-Lancet Commission, https://www.who.int/initiatives/a-future-for-the-worlds-children.
[90] Special Eurobarometer 566 on 'the Digital Decade' 2025: https://digital-strategy.ec.europa.eu/en/news-redirect/883227.
[91] Health Behaviour in School-aged Children (HBSC) international report from the 2021/2022 survey presented in 2024, updated every four years, in collaboration with the WHO Regional Office for Europe. A focus on adolescent peer violence and bullying in Europe, central Asia and Canada. Health Behaviour in School-aged Children international report from the 2021/2022 survey. Volume 2.
[92] Ibid, Volume 6. A focus on adolescent social media use and gaming in Europe, central Asia and Canada: Health Behaviour in School-aged Children international report from the 2021/2022 survey.
[93] Boniel – Nissim M et al., International perspectives on social media use among adolescents: Implications for mental and social well-being and substance use, 2022.
[94] Better Internet for Kids – Review of year 2024. Available at: https://better-internet-for-kids.europa.eu/en/about/insafe-inhope.
[95] Children's Internet. Report on monitoring the presence of children and young people on the Internet. 2025 (in Polish).
[96] Joint Research Centre, Cabeza Martínez, Begoña and d'Hombres, Beatrice and Kovacic, Matija, Social Media Use, Loneliness and Emotional Distress Among Young People in Europe (January 09, 2025). Ca' Foscari University of Venice, Department of Economics Research Paper Series No. 01/2025, Available at SSRN: https://ssrn.com/abstract=5089729. The paper uses survey sample from people aged 16-35.

Audiovisual Media Services Directive[97]; the General Data Protection Regulation (GDPR)[98]; the **Better Internet for Kids strategy (BIK+);** and the EU-co-funded network of **Safer Internet Centres in Member States** which reached over 35 million users in 2024. The **EU AI Act** is also relevant in this area, as it bans AI systems that exploit children's vulnerabilities and requires additional safeguards for high-risk applications affecting minors. The protection of minors is one of the enforcement priorities of the Commission under the DSA. In 2024 the Commission opened four formal **DSA enforcement** proceedings related to minors—one each against Meta's platforms, Facebook and Instagram, and two involving the provider of TikTok, one of which led to the suspension of addictive features in TikTok Lite and ultimately to the removal of that programme with a binding commitment not to re-launch it. In May 2025 the Commission opened formal proceedings against Pornhub, Stripchat, XNXX, and XVideos which also focus on the risks for the protection of minors, including those linked to the absence of effective age verification tools.

To continue protecting children into the future, the EU is preparing **guidelines under the DSA** to help online platforms ensure a high-level of privacy, safety and security for children using their services. These guidelines are expected in 2025 and will also help national authorities responsible for the enforcement to consistently apply rules for the providers of platforms below the threshold of 45 million monthly active recipients. In parallel, the Commission is developing a **short-term, privacy-preserving age-verification solution,** before EU Digital Wallets are offered to EU citizens and residents by the end of 2026. The Commission will also launch an **enquiry into the impact of social media on the mental health** of minors and is preparing an **action plan against cyberbullying**. Moreover, the upcoming evaluation of the Audiovisual Media Services Directive due by December 2026, accompanied where appropriate with proposals for its review, will assess the impact of this Directive and its added value when it comes to the provisions relating to the protection of minors against harmful content. Concerning the GDPR, the European Data Protection Board continues to work on guidelines about processing of children personal data expected to be finalised in 2026.

Protecting children - Recommended policies, measures and actions

Member States should:

- *implement the harmonised EU age-verification solution in the national EUDI Wallets, including systems for issuing the proof-of-age attestations, and accelerate the issuance of electronic means of identification to minors;*
- *take action to ensure the protection of minors and their well-being online, by cooperating on important issues such as age verification and cyberbullying, including through support for the future action plan against cyberbullying.*

d. Preserving information integrity

In 2024, disinformation, often driven by manipulative social media algorithms, continued to undermine trust in institutions and democratic processes. The EU faces rising threats from coordinated inauthentic behaviour (CIB) and foreign information manipulation and interference (FIMI), with fake accounts, bots, and troll farms distorting public discourse and simulating grassroots

[97] In particular the provisions on protecting minors against harmful content (Articles 6a and 28b) and the requirement to adopt appropriate measures to that end, including through age verification.
[98] GDPR states that processing of children personal data merit special protection. For example, the GDPR provides for explicit requirement to use child-friendly language and provides for rules on age of consent for information society services.

sentiment - frequently as part of state-sponsored influence operations. Nearly 50% of EU citizens report encountering false or doubtful content online, reaching over 70% in the Netherlands[99].

In response, the Commission has taken strong action, in particular by endorsing the integration of **the Code of Practice on Disinformation into the framework of the DSA, as a Code of Conduct** under Article 45 of the DSA, entering into application by July 2025. The Commission has launched four formal proceedings against the providers of major platforms Meta, TikTok and X, which focus on risk assessment and mitigation in the area of information manipulation.

The Commission also continues to support the **European Digital Media Observatory**, including its 14 fully operational hubs covering the entire EU. A **Creative Europe** call in October 2024 funded cross-border media literacy projects.

To address the challenges disinformation presents to elections, the Commission has used a wide toolbox, including the recommendation on protecting the integrity and resilience of the electoral process[100], the European Cooperation Network on Elections and the joint election resilience mechanism, made available to support Member States' authorities in building their capacity to detect and react appropriately to threats[101]. In the context of the DSA, targeted action has been taken through expert missions, stakeholder roundtables and stress tests, with the involvement of the Commission, Member States and Digital Services Coordinators (DSCs). In March/April 2024 the Commission published guidelines on recommended measures to the providers of VLOPs and VLOSEs to mitigate systemic risks online that may impact the integrity of elections[102]. A **DSA Toolkit**[103], published in February 2025, offers national regulators best practices in their work with the providers of VLOPs and VLOSEs to mitigate electoral risks, including in relation to hate speech and manipulation. In December 2024, the Commission opened formal proceedings against the providers of TikTok under the DSA for suspected failure to mitigate risks to election integrity in Romania.

Mechanisms under the **Code of Practice on Disinformation** such as the **Rapid Response System** (RRS), active during EU and national elections[104], enabled real-time fact-checking and content flagging in 2024 and continue to do so in 2025. The **European Digital Media Observatory** (EDMO) provided daily briefs and trend insights throughout the year.

In 2024, the EU has also introduced new EU common standards in the internal market. They will enable citizens to easily recognise **political advertising**, understand who is behind it and know whether they have been targeted[105]. Such rules address the growing complexity and cross-border nature of political advertising in the internal market, its growth in the online space, the use of advanced targeting techniques and the threat of information manipulation and interference.

---

[99] Indicator Evaluating data, information and digital content (2021 onwards), Eurostat: isoc_sk_edic_i21, year 2023.

[100] Commission Recommendation (EU) 2023/2829 of 12 December 2023 on inclusive and resilient electoral processes. It includes different recommendations on protecting the integrity and resilience of the electoral process. For example, it encourages Member States to take measures to protect the information environment around elections and ensure that voters receive correct information. It recommends building resilience and developing public awareness, media literacy and critical thinking to address information manipulation, interference and disinformation related to elections. It also calls on Member States to develop training to relevant authorities and to facilitate cooperation among relevant stakeholders to tackle the information manipulation risks.

[101] In the context of this network, Member States discussed practical solutions to a range of threats including FIMI and disinformation. One of the operational tools is the joint election resilience mechanism, which supports exchanges among Member State experts, which several Member States used in the run-up to the elections.

[102] European Commission, Commission publishes guidelines under the DSA for the mitigation of systemic risks online for elections. Available at: https://digital-strategy.ec.europa.eu/en/news/commission-publishes-guidelines-under-dsa-mitigation-systemic-risks-online-elections

[103] European Commission, Commission presents new best-practice election toolkit on the Digital Services Act. Available at: https://digital-strategy.ec.europa.eu/en/news/commission-presents-new-best-practice-election-toolkit-digital-services-act

[104] See the Commission's Report on the 2024 elections to the European Parliament (publication pending at the time of writing).

[105] Regulation (EU) 2024/900 on the transparency and targeting of political advertising.

Fostering the EU's media ecosystem has been a priority. The role of free and independent media is crucial to address the current disruptions in the information space, fostering a pluralistic public debate. However, the news media sector in Europe is undergoing a profound transformation due to market disruptions, uneven access to content, emerging threats to media pluralism, and new funding challenges related to the evolving geopolitical landscape. The **2024 Media Pluralism Monitor**[106] reports a medium risk to fundamental protection of media (average score: 34% in the EU) and a high risk to market plurality (67% in the EU), driven by ownership concentration and lack of transparency in online content removal. To deal with challenges in the media market, the **European Media Freedom Act**[107] was adopted in 2024.

Looking ahead, the **European Democracy Shield** will, among other things, strengthen societal resilience and preparedness, and foster citizen participation and engagement. It will support free, pluralistic and independent media, and look at ways to reinforce our collective capacity to prevent, detect, analyse and respond to foreign information manipulation and interference (FIMI) and disinformation, including when they impact elections and voting behaviours, regulatory processes and public decision-making processes.

Preserving information integrity - Recommended policies, measures and actions

Member States should:

- *increase resilience against disinformation by investing in areas such as fact-checking, media literacy and technological detection tools;*
- *promote further research on information manipulation, looking into the structural, economic, psychological, and technological factors that contribute to its spread;*
- *develop and implement national strategies for countering foreign information manipulation and interference, including improved detection, response capacity, and secure information exchange channels;*
- *develop new strategies to ensure a pluralistic media sphere, including through financing provisions for news media, in ways that respect media independence.*

4. Harnessing digitalisation for the green transition

a. The digital-green nexus: unlocking sustainability, competitiveness and sovereignty

Digitalisation and environmental sustainability are no longer parallel priorities – they are **mutually reinforcing transformations**. If deployed effectively, digital solutions could cut **15 - 20% of global greenhouse gas emissions** by 2030, notably through improved efficiency in buildings, energy, transport, and manufacturing sectors[108].

This digital-green nexus also enhances Europe's industrial competitiveness. Greener digital infrastructure and smart technologies reduce operational costs and encourage adoption by consumers. The integration of AI and the internet of things into energy and resource management enables more efficient operations, particularly for SMEs and municipalities. This contributes to

[106] Centre for Media Pluralism and Media Freedom, Technical Report, EUI, RSC, Research Project Report, 2024. Available at: Monitoring media pluralism in the digital era: application of the media pluralism monitor in the European member states and in candidate countries in 2023.
[107] Regulation (EU) 2024/1083 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act).
[108] Joint Research Centre European Commission, 5 digital solutions for a greener Europe, 2023.

decarbonisation while strengthening Europe's position in emerging green tech markets. Not only do digital tools optimise supply chains, but they also enable circular and profitable business models (such as Product as a Service).

Digitalisation for smart greening is critical to increase Europe's strategic autonomy and resilience. Digital tools such as smart metering allows better demand-side energy management and currently encompasses approximately 60% of European households on average. Nonetheless, substantial disparities persist between EU member states[109]. The launch of the code of conduct for energy-smart appliances will enable interoperability and boost the participation of smart appliances in demand response schemes. Climate observation satellites and predictive analytics contribute to **early warning systems and help manage climate-related risks** such as floods, wildfires, and droughts. As demand for low-carbon infrastructure and advanced computing grows, control over foundational technologies - including semiconductors, secure data infrastructure, and energy-efficient data centres - —has become a critical factor in reducing strategic dependencies.

AI is increasingly seen as a game changer for the green transition. When deployed responsibly, AI enables significant emissions reductions by improving energy efficiency, streamlining industrial processes, and supporting smarter resource management across sectors such as energy, transport, and agriculture. The potential of AI is amplified when combined with digital twins, sensor networks, and data-driven systems. The deployment of the energy data space will unlock consistent, high-quality and interoperable energy data for the training of AI models for energy and the inception of innovative energy services. The Smart Energy Expert Group was launched in October 2024 to support the establishment and governance of this initiative, through its 'Data for Energy' sub-group. AI-enabled decentralised energy systems, smart grid optimisation, and digital twins of the European electricity grid are helping improve energy efficiency and reduce reliance on imported fossil fuels. For example, AI-based grid management will be able to reduce electricity transmission losses while improving load balancing in real time[110]. Nevertheless, **AI's own environmental footprint–particularly that of Generative AI**–must be addressed, especially the energy-intensive and water-intensive nature of training AI models. With global electricity demand from generative AI projected to reach up to **134 TWh by 2027**, comparable to the annual consumption of Sweden[111], aligning AI development with climate goals is essential.

b. Rising pressures: electricity and water demand in the digital transition

Despite the potential advantages of digitalisation for the green transition, the environmental footprint of the digital economy is rising. In 2024 data centres in Europe consumed approximately **70 terawatt-hours (TWh)** of electricity. While this accounts for about **2% of total electricity consumption in Europe**, for some countries, such as Ireland, electricity consumption by data centres is significantly higher, reaching 20% of total consumption. By 2030, electricity consumption by data centres in Europe is expected to grow by **over 45 TWh**, reaching a total of **approximately 115 TWh**. This constitutes a **70% increase** over 2024 levels[112]. While data centres are important consumers of energy, they also offer an opportunity to contribute to system flexibility and demand response. Under the right conditions, they have the potential to provide grid services through the use of on-site battery storage, flexible cooling systems, load shifting, or by relocating computing workloads from one region to another as a form of sustained curtailment.

[109] European Union Agency for the Cooperation of Energy Regulators, Country Sheets : Monitoring data 2023, 2024.
[110] International Energy Agency (2023), Digital Demand-Driven Electricity Networks Initiative, 2024.
[111] McKinsey & Company, The Economic Potential of Generative AI: The Next Productivity Frontier, 2023.
[112] IEA, AI and Energy,2025.

It is forecast that mobile networks alone are expected to consume up to **170% more energy by 2026**, driven by the expansion of 5G networks[113]. Generative AI, AI training and inference, high-performance computing, and edge networks are further accentuating these trends.

In parallel, **water use for cooling digital infrastructure is becoming a growing concern**. The water needed to produce semiconductors is significant. In addition, depending on the cooling method and local climate, data centres can require substantial amounts of water, particularly when using evaporative cooling systems[114].

The rapid deployment of AI accelerators and dense compute clusters exacerbates this challenge. Studies show that by 2027, global AI demand could consume between 4.2 and 6.6 billion cubic metres of water a year[115]. Both the water and electricity consumption of data centres will be a key issue that the Commission will address through the forthcoming follow-up to the Energy Efficiency Directive and the Cloud & AI Development Act.

c. Recent EU actions supporting the green digital nexus

Since 2024, the European Commission has intensified its efforts to promote synergies between digital, energy, climate and circular economy actions. For example, the work on the **EU Code of Conduct for sustainable telecommunications networks** is advancing, with exchanges on a new draft occurring at a stakeholder workshop in May 2025.

In January 2025, the Commission adopted a new delegated regulation for establishing an EU-wide scheme to rate the **sustainability of EU data centres**, requiring operators of data centres above 500 kW to report key performance indicators to the European database by covering–among other things– energy use, water consumption, heat reuse and the type of refrigerant used. This lays the groundwork for more transparency on the sustainability performance of data centres that could be sought by future policy decisions.

In addition, the **Water Resilience** Strategy, launched in March 2025, provides guidance on water-efficient cooling technologies and supports municipalities hosting digital infrastructure through funding instruments under Horizon Europe and LIFE. The forthcoming **Digital Product Passport** framework will also apply to ICT equipment, detailing their environmentally relevant information. This will ensure lifecycle emissions and repairability are factored into procurement decisions.

The **European Green Digital Coalition** is a grouping of companies that seeks to harness the emission-reducing potential of digital solutions for all other sectors of the economy. With the support of the Commission, the European Green Digital Coalition released in 2024 a methodology to assess whether a deployed digital solution reduces more emissions than the solution's own carbon footprint. The Coalition will assess in 2025-2026 another 50 digital solutions in the sectors of energy, transport, construction, smart cities, manufacturing, agriculture and healthcare. It will also work with financial institutions to help sustainable finance to scale the deployment of such green digital solutions.

The twin green and digital transition measures at Member States level

In 2024, a wave of activity began operationalising the twin green and digital transition[116] through national strategies, regulations, and sectoral deployments. This marked a shift from high-level ambitions to systemic policy implementation that jointly advances digital transformation and

[113] GSMA, Energy Efficiency in Mobile Networks: A Roadmap to 2030, 2023.
[114] Circular water solutions key to sustainable data centres | World Economic Forum.
[115] Islam M.A. , Li P., Ren S., Yang J.,Making AI Less "Thirsty": Uncovering and Addressing the Secret Water Footprint of AI Models, 2023.
[116] European Commission, The twin green & digital transition, 2022.

environmental objectives. Measures such as **Italy's Transition 5.0 Plan**, **Luxembourg's National Energy Data Platform**, and **France's Frugal AI standard** illustrate how EU support has been translated into localised, impactful action. The revised Digital Decade **National Roadmaps** include 67 measures from 19 Member States contributing simultaneously to the Digital Decade's green and digital objectives. Of these 67 measures, 38 are specifically designed to simultaneously address those green and digital objectives, with a total investment of EUR 214.2 million.

Best practice highlights

France is leading the Green IT Cluster of the Best Practice Accelerator, and it has put forward three best practices on the twin transition field in 2024: (i) the **General Policy Framework for the Eco-design of Digital Services** , which targets ICT professionals and sets out 78 criteria and best practices applying eco-design principles in the development of services and the drafting of an Eco-design Declaration; (ii) the development and availability of **Product Category Rules** (PCR) for environmental evaluation and labelling to improve the environmental information provided to consumers, covering the entire product life cycle; and (iii) **the Alt IMPACT Communication Campaign** to raise public awareness about the environmental impact of digital technologies.

The Netherlands presented its **Sustainable Digitalisation Action Plan** published in July 2024. It outlines 44 concrete actions across three main pillars that work towards making the digital sector more sustainable, while simultaneously leveraging digitalisation for sustainability by improving the efficiency of production processes, optimising the use of existing resources, and enabling the circular use of raw materials and resources.

Finland presented a set of measures to increase the **knowledge base on the environmental handprint and footprint of the ICT Sector**. This set of best practice measures was in response to the lack of reliable and comparable data identified as one of the challenges during the drawing up of its national climate and environmental strategy for the ICT sector, which Finland published in 2021.

Luxembourg presented its **Product Circularity Data Sheet (PCDS)**, a tool designed to provide detailed information about the circular characteristics of products, such as their recyclability, their durability, and their use of recycled materials. The PCDS is aligned with the general and cross-cutting requirements of the Ecodesign for Sustainable Products Regulation.

Harnessing digitalisation for the green transition - Recommended policies, measures and actions

Member States should:

- *support the development of harmonised environmental impact metrics for digital solutions including AI-based solutions as well as metrics for digital infrastructures such as, edge computing, data centres, and telecommunications networks;*
- *reinforce their cooperation with the AI Office, the Green Digital Coalition, and the European Green Deal Data Space, as well as contributing to the upcoming EU Code of Conduct for sustainable telecommunications networks;*
- *incorporate digital sustainability KPIs into their national digital and green transition plans.*

5. Building coherence, efficiency and simplification

In 2024, the Commission made a strong commitment to an ambitious simplification agenda[117], presented in the Communication on a Simpler and faster Europe[118]. The Digital Decade is aligned with this simplification approach and includes a joint commitment to ensure that digital policies, measures, and programmes relevant for the EU's digital transformation are considered in **a coordinated and coherent way** so that they fully contribute to the Digital Decade objectives, while **avoiding regulatory overlaps and minimising administrative burdens.**

a. Need for simplification, efficiency and coherence

i. Better and lighter digital legislation

In 2024 and through 2025, the Commission prioritised the streamlining of EU legislation to enhance competitiveness, minimise the burden of compliance, reduce red tape and streamline regulation to ensure consistency. More than half of European SMEs flag such regulatory and administrative obstacles as their greatest challenge[119]. 86% of EU firms dedicate staff to compliance tasks, with the cost of compliance averaging 1.8% of turnover—rising to 2.5% for SMEs[120]. This is a similar order of magnitude to average energy costs, standing at 4% of annual turnover.

The **Commission has set an overarching target to reduce reporting burdens** by at least 25% for all companies —and by at least 35% for SMEs – before the end of its current mandate, without undermining the policy objectives of the reporting rules.

For the digital *acquis*, the Commission is planning **a wide 'stress test' of the regulatory framework.** Over the coming years, this stress test will include an assessment of regulatory coherence and whether the current rules are fit for purpose considering the rapid technological transformation and market evolution. The stress test will also explore whether further reductions can be made to the reporting and compliance burden, while pursuing the objectives of the regulations.

Firstly, in May 2025, the Commission came forward with the **Single Market Simplification** proposal. The Fourth Omnibus package simplifies the record-keeping obligation in the GDPR, taking into account the specific needs and challenges of small and medium-sized companies and organisations, while ensuring that the rights of individuals are protected.

Looking forward, in the fourth quarter of 2025, the Commission will put forward a **Digital Package**, including a Digital Omnibus proposal with a series of simplification measures for part of the digital *acquis*, stress-tested over the year.

In addition, the European Commission plans to propose the **Digital Networks Act**. This forthcoming legislation will transform Europe's digital infrastructure to support European businesses and citizens in an increasingly connected world. This effort is fully aligned with the broader priorities of the Competitiveness Compass, where digital infrastructure is fundamental to Europe's leadership in innovation, resilience, and long-term economic growth. At the core of this initiative is simplification. The Digital Networks Act will reduce regulatory burden, provide clarity, strengthen competition, all while safeguarding consumer benefits. The Digital Networks Act will ensure that digital infrastructure is built for the future.

[117] European Commission, Simplification and implementation. Available at: https://commission.europa.eu/law/law-making-process/better-regulation/simplification-and-implementation_en.
[118] European Commission, A simpler and faster Europe, 2024.
[119] Draghi, M., The future of European competitiveness, Part A – A competitiveness strategy for Europe, pg.14 2024.
[120] EIB Investment Report 2024–2025, European Investment Bank.

The **transformative potential of digital tools for administrative simplification** has been strongly endorsed by recent high-level reports on competitiveness. The Commission is leading efforts to build a dedicated infrastructure modelled on **Common European Data Spaces to automate regulatory compliance and data transmission.**

The **European Business Wallet** will be a cornerstone of doing business simply and digitally in the EU, providing a seamless environment for companies to interact with all public administrations is the upcoming European Business Wallet. Building on the EUDI Framework, the European Business Wallets will be horizontal enablers for Europe's competitiveness. The European Business Wallets are intended to streamline business-to-business and business-to-government interactions, enabling trusted digital identities, secure data exchanges and legally recognised digital notifications. It will reduce administrative burdens, lower compliance costs, and enhance cross-border transactions, benefiting SMEs and large enterprises. By streamlining processes, it will also improve business efficiency and foster competitiveness.

Alongside this, the **Single Digital Gateway** (SDG), and its cornerstone component -the **Only-Once Technical System** (OOTS) -could automate the exchange of verified data between public authorities, cutting administrative costs for SMEs by over 50%, according to a 2024 impact study[121]. By 2025, most Member States are expected to be technically ready to securely exchange official documents across borders, increasing the accessibility and interoperability of e-Government services for around 80 000 national authorities. Despite progress in this area, challenges remain - particularly in digitising industrial permitting procedures essential for sectors like renewable energy and semiconductors. Although EU legislation such as the SDG Regulation, the Net Zero Industry Act, and the Critical Raw Materials Act provide a strong legal foundation for the digital and green transitions, disparities persist as many Member States still lack the organisational and digital capabilities to fully implement and benefit from these reforms.

Further integration of these systems is planned. The **European Business Wallet, EU Digital Identity Wallet, SDG and OOTS will together form a cohesive, interoperable digital infrastructure**. This ecosystem will enable seamless interactions for businesses and citizens and reduce duplication in compliance processes. However, the slow progress made by national and local entities in implementing OOTS and the SDG remains a challenge, and this progress requires targeted alignment efforts and shared procedural standards.

EU company Law will reduce burden on companies leveraging digital solutions in synergy with the European Business Wallet, and through the Business Registers Interconnection System (BRIS) that enables the 'once only' principle with regard to company data. The '28th Regime' proposal will further support companies to set-up and grow in the EU, making it possible for innovative companies to benefit from a single, harmonised set of EU-wide rules wherever they invest and operate in the single market, as announced in the Competitiveness Compass. The digital euro initiative is also contributing to simplification. By ensuring interoperability **with the EU Digital Identity Wallet**, the Commission aims to provide users of the digital euro with a streamlined and secure means of verifying identity, confirming payments, and facilitating offline transactions. This will reduce transaction costs, especially for SMEs, and strengthen Europe's digital sovereignty.

Another major milestone was the adoption of the **VAT in the Digital Age** legislative package on 11 March 2025. This enables automated VAT reporting through e-invoicing, simplifying data extraction

[121] European Commission, EU SMEs and self-employed workers could save time and money when expanding abroad thanks to the once-only technical system, 2024.

and supporting sustainability reporting. Exploratory work is underway to align this functionality with the European Financial Reporting Advisory Group (EFRAG)'s sustainability standards, using e-invoices to meet environmental reporting obligations efficiently.

ii. Simplification through improved governance

Ensuring the effectiveness of this comprehensive simplification agenda requires improved governance. The **Digital Decade Board (DDB) has emerged as the primary forum for coordination** between the Commission and Member States on digital policy implementation. With a broad mandate, the DDB brings together national representatives to align digital measures, share best practices, and assess emerging challenges in the regulatory landscape.

The DDB has discussed several **avenues to reduce administrative burden**: (i) simplification through digital tools; (ii) the setting up of a Digital Single Rulebook;(iii) the setting up of a Single Digital Compliance Platform or (iv) codifying compliance requirements into a single interface. There are also some possible synergies regarding overlaps and fragmentation across the Commission's expert groups, which may exceed the administrative capacity of national authorities. As a first step, the Commission is conducting an **overview of all advisory bodies linked to digital legislation** to support internal coordination within Member States and improve strategic alignment. The potential streamlining of these structures will in particular be considered as part of the 2026 review of the Digital Decade Policy Programme (DDPP).

Coherence and simplification - Recommended policies, measures and actions

Member States should fully leverage the DDB's role and expertise to help streamline the implementation of digital acquis and support the development and deployment of solutions for simplification and reduction of administrative burden.

b. Funding the Digital Decade

The priority given to the digital transition by the Commission is reflected in the EU budget's commitment. Nearly all EU programmes contribute to digital goals, with key focus areas including the **digitisation of public services**, **digital skills**, **business digitalisation**, **advanced digital infrastructure** (such as 5G, AI, quantum, and cloud technologies), and **support for research and innovation**. Health and transport are two other major sectors targeted for digital transformation[122].

The Joint Research Centre (JRC)[123] study on five major programmes—**RRF, CEF Digital, Horizon Europe, DIGITAL, and Cohesion Policy**—estimates that between 2020 and 2027, a total of **EUR 207 billion** in public money will support digital objectives. Of this, **EUR 177.5 billion** directly contributes to achieving the EU's **Digital Decade targets**. The **RRF** alone accounts for over **EUR 149.8 billion** in public digital investments, with **EUR 135.7 billion** directly aligned with the targets, making it the single most significant contributor to digital investments in the EU[124]. It plays a leading role in promoting **basic digital skills**, the training of **ICT specialists**, **gigabit network coverage**, **digital public services**,

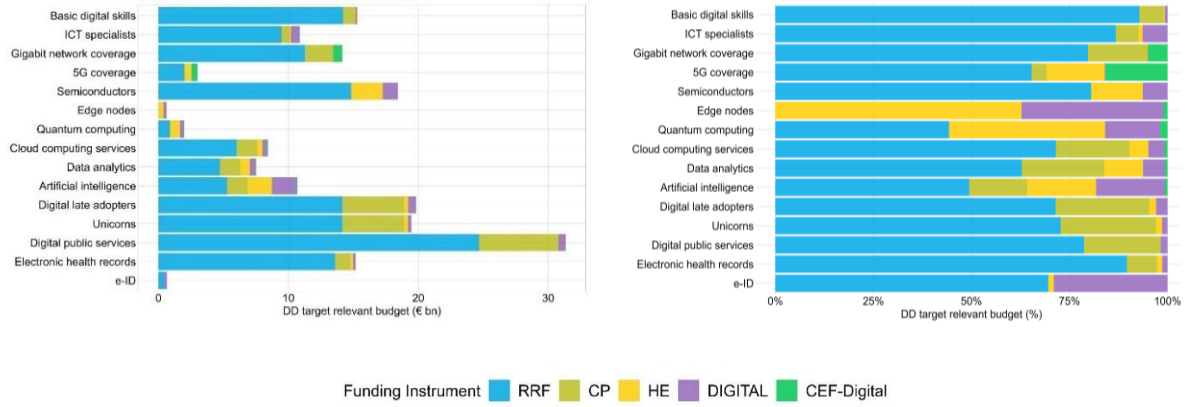
[122] The latest stocktaking exercise referred to EU spending from 2021 to 2023 shows that approximately EUR 205.5 billion—around 17.5% of the total EU budget—was dedicated to the digital transition. A significant portion of this funding was mobilized through the Recovery and Resilience Facility (RRF), which in the same period allocated 24% of its total budget to digital investments and reforms. Available at: https://commission.europa.eu/strategy-and-policy/eu-budget/performance-and-reporting/horizontal-priorities/digital-tracking_en

[123] Joint Research Centre, Nepelski, D. and Torrecillas, J. Mapping EU level funding instruments 2021-2027 to Digital Decade targets – 2025 update, Publications Office of the European Union, Luxembourg, 2025, JRC141966.

[124] Including measures in the Repower EU chapters contributing to the digital transition. Last update on 10 March 2025.

semiconductors, and **eHealth**, contributing over 70–90% of the relevant funding in each of these areas.

Figure 1: Relevant budget by funding instrument and Digital Decade target, in billion EUR (on the left) and as % (on the right)



Source: JRC Calculations

In addition to public funding, mobilising private investments plays a crucial role. The EU is increasingly using its budget to support private digital investment through tools such as **InvestEU**, **Joint Undertakings (JUs)**, and **Public-Private Partnerships (PPPs)**. As of March 2025, **InvestEU has mobilised EUR 15.88 billion** in digital-related investments. However, financial instruments are not yet fully taken advantaged of in all programmes[125] and often lack a strong policy steer or the scale needed to address systemic investment gaps. **Blending instruments and guarantees (e.g. InvestEU) show promising results in this area.** Depending on the level of technology readiness, **leveraging factors** from financial instruments (i.e. the amount of private money that is invested alongside every euro of public money) are currently **around 3 for early-stage deep-tech** companies (European Innovation Council Fund equity) and **around 5.62 from the InvestEU guarantee**[126]. **Overall, the EU faces a substantial and urgent need to increase investment in digital technologies, infrastructure, and innovation ecosystems.** Bridging the investment gap, estimated in the hundreds of billions annually, requires not only more funding, but smarter, better-targeted financial instruments, deeper capital markets, and stronger coordination across EU and national programmes. Strategic public support will remain essential in high-risk areas such as AI, cybersecurity, and deep tech, while effective leveraging of private investment will be key to achieving scale and impact. As Europe prepares for its next **Multiannual Financial Framework (MFF)** and advances its **Digital Decade objectives**, aligning funding with strategic priorities and maximising impact through higher coordination, across programmes and across the EU, will be critical to securing Europe's digital sovereignty and long-term competitiveness.

[125] As an example of needed flexibility, the EIC blended finance allows successful companies to decouple the timing of the grant and equity finance, without the need to go through a new application process when the time is ripe (e.g., when co-investors have been found). See also Mundell, The ecosystem: European Innovation Council uncouples grant and equity funding for startups, 2024. Available at: https://commission.europa.eu/strategy-and-policy/eu-budget/performance-and-reporting/horizontal-priorities/digital-tracking_en.

[126] From the Interim evaluation of the InvestEU Programme (1 October 2024).

Funding the Digital Decade - Recommended policies, measures and actions

Member States should:

- *prioritise strategic digital investment in their national budgets, aligned with Digital Decade objectives, EU Digital Principles, and sovereignty imperatives, including taking action to mobilise private investment;*
- *pursue reforms, including in public procurement, to facilitate the emergence and scaling of sovereign digital technologies and infrastructure;*
- *collaborate actively in the development of large-scale digital projects with transnational relevance, potentially supported by new common financing mechanisms or a dedicated Digital Sovereignty Fund.*

c. Cooperation with cities and regions

In the context of the Digital Decade, the European Commission is strengthening its cooperation with cities and regions, recognising that subnational governments play a pivotal role in implementing and disseminating digital policies that affect businesses, public services, and citizens on the ground.

With over **90 000 local governments** across the EU and EFTA, greater **coordination will be critical** for **digital transformation to scale**, to avoid duplication, improve interoperability, and share knowledge and digital infrastructure. Although innovation clusters and large cities are accelerating their digital transition, many smaller municipalities and rural areas are falling behind. To accelerate the dissemination of digital technologies across the EU and bridge the divide between innovation hot spots (typically in large cities) and the smaller cities that often lag behind, cities must be seen not just as implementers of policy made elsewhere, but as **strategic partners** building on their proximity to citizens and SMEs.

In this context, the **Digital Decade Policy Programme (DDPP) offers a valuable opportunity and framework for cities to align digitalisation** with wider priorities such as climate action, mobility, housing, and social inclusion. The DDPP also contributes as a strategic framework to the upcoming Commission **policy agenda for cities**, initiated at the start of the new mandate.

Aligning digitalisation with wider priorities will require accurate and timely data aligned with the Digital Decade targets and objectives. In 2024, the EU's **LORDIMAS monitoring** tool allowed self-assessments from **99 regional, metropolitan, and local administrations**, offering insights on EU digitalisation at subnational level. As of March 2025, **184 administrations had joined LORDIMAS**, with continued outreach to expand participation. This effort complements other initiatives, such as the **LDT-CitiVERSE** (see above), **Living-in.EU** and **Local Observatories** that are developed by cities to track digital progress and better target investment, especially in areas like **urban resilience, and bridging the digital divide.**

Cooperation with cities also includes the set-up of digital ecosystems that integrate skills development, connectivity infrastructure, and support for enterprises, especially SMEs. **European Digital Innovation Hubs (EDIHs)** and **AI Testing and Experimentation Facilities (TEFs)**, such as **CitCom.ai**, offer cities and local actors the tools to test and deploy emerging technologies in real-world conditions. CitCom.ai, launched in January 2025 with EUR 40 million in EU co-funding, is already trialling AI applications in smart mobility, energy, and urban planning across **11 EU countries**. The Commission also continues to support cities' connectivity through targeted investment in **high-speed**

broadband, **5G**, and **fibre infrastructure**. Over **7 200 municipalities** have benefited from **WiFi4EU**, an EU-funded programme to deliver free wifi to towns and villages across Europe, improving access to connectivity in remote areas.

Cities are also key actors in upholding the **European Declaration on Digital Rights and Principles**. Local initiatives such as the **Brussels Digital Rights Charter** and **Leipzig's Hardware for Future** project reflect the values of **equity, transparency, and citizen empowerment**. The **Cities Coalition for Digital Rights**, supported by the Commission, helps scale and replicate such efforts across Europe.

Best Practice: Portugal's Smart Territories National Strategy (ENTI)

*Portugal's **ENTI**, launched in August 2024, offers a compelling model for digital development. Funded with **EUR 60 million** from the Recovery and Resilience Facility, it integrates **digital twins, real-time data platforms, and urban dashboards** to improve regional development, public service delivery, and environmental monitoring. Rooted in EU digital rights and sustainability principles, it sets a benchmark for **data-driven, inclusive, and green territorial governance**.*

Cooperation with cities and regions - Recommended policies, measures and actions

Member States should:

- *encourage cities to participate in multi-country projects such as the LDT-CitiVERSE-EDIC and support cross-border reuse of digital public services;*
- *anchor local digital strategies in the European Declaration on Digital Rights and Principles (DRP);*
- *invite cities to adopt their own local Digital Rights and Principles Charters;*
- *invest in local digital capacity and data-driven governance: foster the development of local observatories (e.g. to monitor the digital divide) and encourage participation in tools to improve data availability and inform targeted policymaking.*