EUROPEAN
COMMISSION

Brussels, 3.11.2026
COM(2026) 288 final/2

ANNEX 1

CORRIGENDUM
This document corrects document COM(2026) 288 final, adopted on 17.6.2026. Concerns all language versions. It concerns corrections in some figures.
Replacement of figure 3 table on page 6 of the Communication document of VHCN for DESI 2026 and 4-year progress:

1. New VHCN 85.6%, replaced value: 85.5%

2. 4-year progress new value 22.8%, replaced value: 22.7%

The text shall read as follows:

ANNEXES

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 2026 Closing structural gaps and mobilising investments for 2030 and beyond

{SWD(2026) 154 final} - {SWD(2026) 155 final} - {SWD(2026) 156 final} - {SWD(2026) 157 final}

European Commission

State of the Digital Decade 2026:

State of EU digital transformation in 2026

Progress and EU-level recommendations

3. Contents

1. Introduction 3

2. Reinforcing technological sovereignty, digital leadership, security and competitiveness 8

2.1. Cutting-edge technological capacities 8

2.1.1 Semiconductors 9

2.1.2 Quantum 13

2.1.3 High-performance computing, AI Factories and AI Gigafactories 16

2.1.4 Edge nodes and computing capacity deployment 17

2.2. Supporting innovative companies with digital tools and resilient network 24

2.2.1. Connectivity 24

2.2.2. Digitalisation of SMEs and uptake of digital technologies by EU enterprises: AI, Cloud and data analytics 38

2.2.3. Open Source 47

2.2.4. Unicorns 49

2.3. Ensuring security for competitive growth 54

3. Protecting and empowering people, reducing burdens and harnessing digitalisation for sustainability 58

3.1. Digital skills for smart society and competitive economy 58

3.1.1. Basic digital skills 59

3.1.2. ICT Specialists 62

3.1.3. Protecting people, in particular minors, in the online space 65

3.2. Efficient public services and administrative burden reduction 68

3.2.1. European Digital Identity and business wallets 69

3.2.2. Digital Public Services for Citizens and businesses 70

3.2.3. e-Health 74

3.3. Digital for decarbonisation and sustainable technologies 78

3.3.1. Sustainable digitalisation for competitiveness, resilience and net positive impacts 78

3.3.2. Rising environmental concerns: electricity, water and material demand for digital transition 79

3.3.3. EU actions to unlock the twin green digital transition 80

3.3.4. Member State actions towards the twin green and digital transition 82

3.3.5. Reforms and investments needed to accelerate the green and digital transition82

4. Funding the Digital Decade..... 84

5. International 89

1. Introduction

This Annex forms an integral part of the State of the Digital Decade 2026 report. It covers in particular technological sovereignty, security and competitiveness; the protection and empowerment of people; the role of digitalisation in the green transition; and a strengthened horizontal dimension on coherence, efficiency and simplification across policies and instruments. It also includes horizontal recommendations.

Recommendations issued under the Digital Decade policy programme may address all dimensions of the Programme: not only the Digital Decade targets, but also the general objectives set out in Article 3 (e.g. sovereignty, resilience, competitiveness, security, fighting digital divides) taking into account the digital principles and rights of the European Declaration. Each recommendation is intended to be operationalised by Member States through the updated National Roadmaps to be submitted by December 2026, in accordance with the coherence framework set out in Section 4 of the Communication.

Member State-specific recommendations complement these horizontal recommendations and are included in Annex 2. The identification of recommendations takes into account the Member States' performance for these areas (as measured by KPIs or other evidence for areas without KPI) plus a comprehensive policy assessment of the measures taken and/or planned by the Member States for that specific areas informed notably by dedicated bilateral exchanges with administrations, civil society and national regulators taking into account structural factors specific to each Member State, the follow-up to the recommendations issued in 2025 and the measures set out in National Roadmaps with the Programme.

The key objective of the recommendations is to enable collective progress and achievement of DD objectives, requiring two complementary and mutually reinforcing approaches: they address gaps where progress is insufficient, and they leverage strengths identified in a Member State - in line with the cooperative approach of the Programme. Reinforcing and scaling up national strengths can support the European Union as a whole to reach the common Digital Decade targets and objectives (for instance, leadership in technologies which are critical for EU's sovereignty, e.g. AI, semiconductors or quantum).

The Member State-specific recommendations focus on a limited number of structural priorities - about five per Member States, are designed to be actionable and future-oriented, and are prioritised on a scale according to expected impact and relevance in the MS context. This targeted approach ensures that recommendations concentrate on the areas with the greatest potential impact on the basis of its expected contribution to the collective achievement of the Union's Digital Decade objectives and targets.

The recommendations of the State of the Digital Decade report operate alongside the digital dimension of the Country-Specific Recommendations adopted under the European Semester and other relevant documents, such as the CAP recommendations. These instruments are complementary. On the one hand, the Digital Decade recommendations aim at achieving the EU-level targets and objectives for the digital transformation of the EU On the other hand, the European Semester can identify digital-specific shortcomings with macro-economic, employment or social impact and address recommendations about digital reforms and investment needs in these areas. These elements are also mirrored in the Digital Decade analysis and recommendations, where applicable with additional elements. The Digital decade is also focusing on advanced digital infrastructures deployment linked to EU's industrial policy and capacities

(e.g. semiconductors, quantum) and cybersecurity. The two tracks have been prepared in close coordination to ensure consistency and complementarity.

The 2026 horizontal recommendations also build on the assessment of the implementation of the 2025 EU-level recommendations, carried out under Article 6 of the Digital Decade Policy Programme Decision[1] and presented in the accompanying Staff Working Document. Recommendations assessed as showing limited progress in 2025 are carried over in updated form, while areas showing notable or significant progress give rise to recommendations focused on consolidation, scaling and uptake.

The analysis provides a comprehensive overview of the state of play, identifying key areas of progress and acceleration, as well as persistent gaps, structural weaknesses, and emerging risks. It highlights the Union's strengths to build on and pinpoints the main bottlenecks requiring reinforced reforms and public and private investment. It also includes updates on the comprehensive monitoring of the Declaration of digital rights and principles undertaken in 2025. The assessment primarily relies on monitoring through the Digital Economy and Society Index (DESI), complemented by relevant studies, expert analysis and the National Digital Decade Strategic Roadmaps submitted by Member States, with a view to informing targeted policy action, improved coordination and stronger collective delivery.

In parallel to investment and capacity-building efforts, the Union has continued to strengthen the regulatory framework underpinning the digital economy, with a view to ensuring fair and contestable markets. In particular, the Digital Markets Act addresses structural imbalances in platform ecosystems by limiting the ability of large digital gatekeepers to act as bottlenecks and by ensuring that digital businesses have opportunities to grow and innovate and together with users can benefit from greater choice, interoperability and access to digital services across the Single Market.

According to the Digital Decade Eurobarometer 2026, three out of four Europeans believe that the digitalisation of public and private services is making their lives easier. Digital health technologies and green digital technologies (e.g. energy-saving tech) are selected by at least half of the respondents when asked which technologies are likely to have a positive impact over the next ten years.

[1] European Parliament and Council of the European Union, Decision (EU) 2022/2481 of 14 December 2022 Establishing the 2030 Policy Programme "Path to the Digital Decade", OJ L 323, 19 December 2022.

Box: Approach to the 2026 Recommendations

The following sets out the methodology used to identify Member State-specific and EU-level recommended policies, measures and actions under the Digital Decade Policy Programme.

I. Legal basis

The recommendations set out in the 2026 State of the Digital Decade Report are based on the provisions of Decision (EU) 2022/2481 of the European Parliament and of the Council establishing the Digital Decade Policy Programme 2030. The relevant provisions are the following:

Article 3 sets out the general objectives of the Programme, covering, in particular, collective resilience, bridging the digital divide, fostering digital sovereignty, the deployment and the use of digital capabilities, the digital empowerment of citizens, cybersecurity, and a sustainable digital transformation.

Article 4 sets out the digital targets to be achieved collectively by Member States by 2030, covering digital skills, digital infrastructure, the digitalisation of businesses, and the digitalisation of public services.

Article 5 requires the Commission to monitor progress towards the general objectives and the digital targets based on Member States' Key Performance Indicators (KPIs), also compared to Union-level projected trajectories, for each of the digital targets established in close cooperation with Member States.

Article 6 requires the Commission to assess, in its annual Report on the State of the Digital Decade, the progress of the Union's digital transformation against both the general objectives and the digital targets, and to identify significant gaps and shortages and recommend policies, measures or actions to be taken by Member States in areas where progress was insufficient to achieve the general objectives and digital targets.

Article 7 establishes the national Digital Decade strategic roadmaps as the main implementation mechanism through which Member States respond to the recommendations and set out the measures they intend to take to address identified gaps, also taking into consideration the latest country-specific recommendations issued in the context of the European Semester.

II. Scope and main factors informing recommendations

Recommendations may address digital targets set out in Article 4 and general objectives set out in Article 3, taking into account the digital principles and rights enshrined in the European Declaration on Digital Rights and Principles.

The identification of recommended policies, measures and actions draws on multiple factors: the performance of each Member State as measured by the relevant KPIs or, where no KPI data is available on Member State level, by other available evidence; a comprehensive policy assessment of the measures taken and planned by the Member State in the relevant area in their national Digital Decade

strategic roadmap and beyond; structural factors specific to each Member State; the follow-up to recommendations issued in 2025.

Recommendations can address both gaps where progress is insufficient and suggest leveraging existing strengths at Member State level. In line with the cooperative approach of the Programme, reinforcing and scaling up national strengths can support the Union as a whole in reaching the common Digital Decade targets - for instance, leadership in technologies critical for EU digital sovereignty such as artificial intelligence, semiconductors or quantum communications.

Member State-specific recommendations are complemented by the EU-level recommendations set out in Annex 1, which adopt a Union-wide perspective and are addressed to all Member States, as applicable.

III. Prioritisation logic for Member State-specific recommendations

In the 2026 State of the Digital Decade Report, Member State-specific recommendations concentrate on a limited set of structural priorities with the greatest potential to accelerate progress towards the Union's Digital Decade objectives and targets. The recommendations are actionable, forward-looking and presented in an indicative order of priority based on their expected impact and relevance, taking into account the specific national context (see heat map below). This prioritisation is intended to help focus efforts on those areas where reforms, investments and policy measures may have the most significant contribution to Europe's digital transformation.

IV. Reflection of these elements across the 2026 State of the Digital Decade report package

Member State-specific and EU-level recommendations are reflected across 2026 State of the Digital Decade report package as follows:

The **Communication presents the Union-wide assessment of the digital transformation**: it measures collective progress against the Article 4 digital targets and the Article 3 general objectives, analyses the key performance indicators against their 2030 trajectories, and sets out the additional measures and investment priorities to be pursued at Union level.

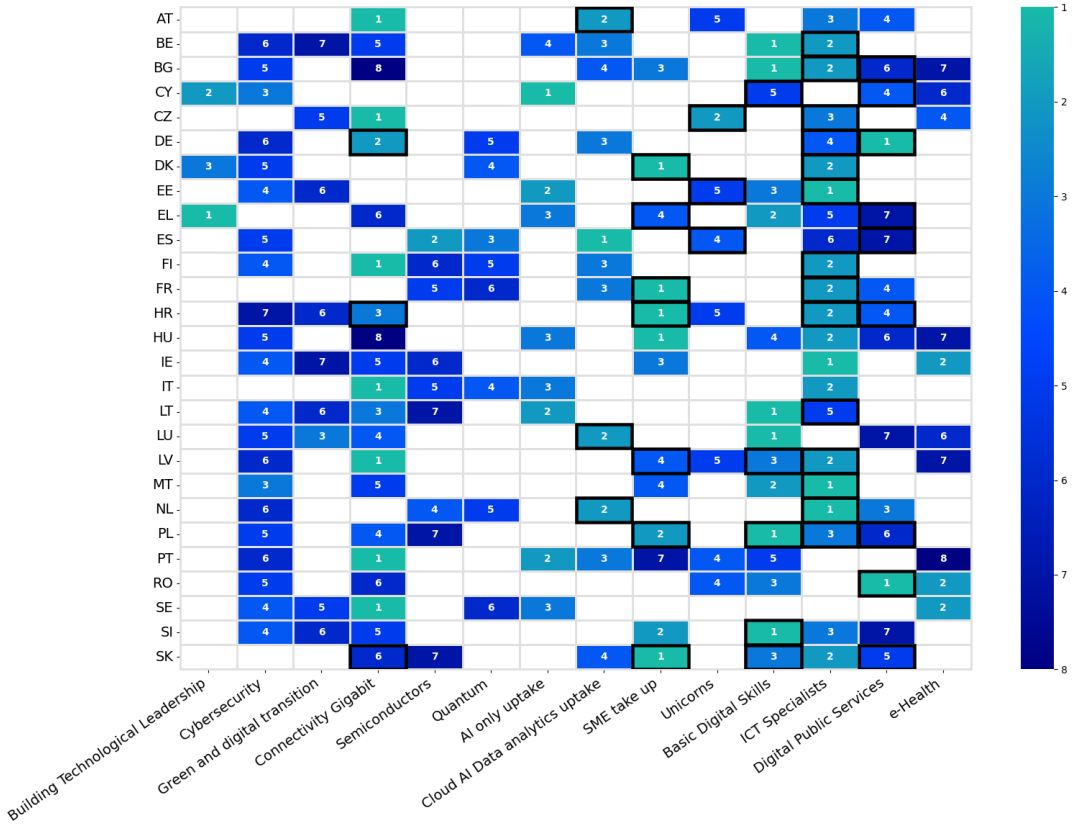
Communication Annex 1 develops this Union-level analysis in detail, presenting the state of play for each target and general objective, together with the EU-level recommendations addressed to all Member States, as applicable.

The country reports (short country reports, including recommendations, are grouped together as Communication Annex 2) translate the assessment to national level. Per Member State, for each thematic area, they are based on an assessment as described under II (see above), including the assessment of 2025 Member-State recommendation progress, which may result in 2026 Member State-specific recommendations.

The Staff Working Document on the monitoring of the 2025 EU-level recommendations reviews the progress made by the Commission and the Member States in implementing the 2025 recommendations grounded in actionable measures such as legislative initiatives, dedicated funding, the adoption of strategies and the implementation of joint projects.

The Staff Working Document on the monitoring of the 2025 EU-level recommendations and the 27 Country reports specifically discharges the Article 6 requirement to report on progress regarding previously recommended policies, measures and actions.

Heatmap of the Member State-specific Digital Decade recommendations and complementarity to European Semester Country-specific recommendations



This heatmap provides an overview of the 2026 Member State-specific Digital Decade recommendations and their relative prioritisation over different policy areas, with regard to their contribution to achieving DD objectives and targets. Cells outlined in black indicate a corresponding country-specific recommendation issued under the 2026 European Semester Spring Package, illustrating the complementarity between the European Semester and the Digital Decade agenda. Please note that the heatmap is structured according to the Digital Decade targets and general objectives only. As a result, the display of European Semester country-specific recommendations should be regarded as illustrative and intended to provide a broad indication of areas of alignment.

2. Reinforcing technological sovereignty, digital leadership, security and competitiveness

The EU's ability to develop, deploy, and maintain control over critical digital technologies is increasingly proving fundamental to its long-term competitiveness, technological sovereignty, and strategic resilience. These dimensions are closely interlinked: sustained productivity gains from digital technologies, particularly AI, can only be secured if Europe reduces its strategic dependencies and strengthens the security of its digital ecosystem. In several critical areas, including cloud computing, advanced computing, semiconductors, and high-performance connectivity, the limited availability of competitive European alternatives continues to constrain substitutability.

This increases risks related both to security of supply and to the jurisdiction applicable to data and services when providers or controllers are not established in the EU. Such dependencies weaken the Union's capacity to regulate and enforce its rules effectively, while exposing key infrastructures and services to external vulnerabilities.

Addressing these risks requires sustained investment in critical technologies, a systematic reduction of strategic dependencies, clear solutions to jurisdiction and enforcement issues for data and services controlled from outside the Union, and robust cybersecurity across the digital value chain - from hardware and infrastructure to applications and services as well as reinforcing international cooperation as appropriate (e.g. to ensure access to markets, secure alternative supply lines, etc). The deployment of critical technologies must be matched by their effective uptake and diffusion across the economy and society, in particular among SMEs, which remain central to unlocking productivity gains and ensuring broad-based benefits from digitalisation. For SMEs and startups to take up opportunities and innovate, rigorous enforcement of the Digital Markets Act is needed to tackle structural imbalances in digital markets, where a limited number of large platforms controls SMEs' access to end users.

While progress has been made in certain areas, the EU continues to underperform globally in several strategic domains. International competitors are consolidating their own sovereignty and leadership through scale, investment and integrated market dynamics, with global leadership in critical technologies increasingly concentrated in the US and China[2]. Bridging these gaps will require reinforced coordination between the Union and the Member States, together with better alignment of reforms, investments and governance frameworks.

2.1. Cutting-edge technological capacities

Europe's ability to compete globally rests on its command of the foundational technologies that underpin modern computing: semiconductors, quantum systems, and edge and computing infrastructures. These

[2] Australian Strategic Policy Institute (ASPI), Critical Technology Tracker, December 2025.

domains are deeply interlinked: advanced semiconductors drive HPC, quantum and edge systems, edge nodes bring computing capacity closer to where data is generated, and quantum technologies promise to redefine computational limits.

Progress across these three areas remains uneven. The EU's share of global semiconductor revenues stands at 8.8%, well below the 20% target set for 2030 in the Digital Decade Decision. Quantum has met its Digital Decade milestone, but deployment is held back by fragmentation and by the scale of investment needed to move beyond NISQ systems[3]. Meanwhile, while edge node deployment is on track to meet the 2030 Digital Decade target ahead of schedule, overall computing capacity still lags significantly behind demand and remains well below US levels.

The stakes attached to these KPIs are both economic and strategic: gaps in these areas translate into critical dependencies on non-EU providers, higher costs for businesses and public services, and a diminished capacity to develop and deploy the next generation of digital technologies on European terms.

A defining trend of 2025-2026 has also been the accelerated integration of digital technologies into European defence capabilities. Digital technologies are no longer peripheral to defence: they increasingly act as core force multipliers, reshaping how capabilities are developed, deployed and integrated across domains. Artificial intelligence, advanced connectivity including in space, cloud computing, cybersecurity tools and autonomous systems, originally developed for civilian applications, are now being systematically adapted for defence purposes, strengthening command and control, situational awareness and electronic warfare. This structural shift from civilian to military innovation, often described as "spin-in", has emerged as a key driver of capability development, and is likely to deepen further as operational lessons from recent conflicts continue to inform technology adaptation and procurement priorities across Member States.

2.1.1 Semiconductors

The global semiconductor race has intensified further over the past year. Chips are at the centre of competitiveness, security and resilience strategies worldwide, as they underpin artificial intelligence, cloud and edge computing, future communications networks, software-defined vehicles, industrial automation, medical devices, defence systems and the wider digital and green transitions. The economic and strategic relevance of semiconductors therefore continues to grow, and with it the pressure on governments to secure access to critical technologies and strengthen trusted supply chains. These dynamics are reshaping the semiconductor market with AI emerging as a pervasive end application. AI-related components are expected to drive growth and account for more than 70% of the total semiconductor market by 2030. Over the past two years, market growth has been driven by chips for AI data centres, notably processors and memory, while most other segments have remained stagnant.

[3] Noisy Intermediate-Scale Quantum (NISQ) refers to current, near-term quantum computers with 50–1000+ qubits, which are powerful but lack full error correction.

The European Union occupies a distinctive position in the global semiconductor ecosystem. Its role is not primarily defined by scale in the most volume-driven segments of leading-edge logic and memory manufacturing, but rather by strong capabilities in strategic parts of the value chain, including equipment, materials, research and technology infrastructures, specialty manufacturing, and semiconductor devices for automotive, industrial, power, sensing and secure applications. This profile reflects the structure of EU industry. The EU hosts leading integrated device manufacturers and specialty foundries, globally relevant equipment and materials suppliers, and major research organisations. As a result, it plays an enabling role well beyond its own regional demand, especially in applications where reliability, energy efficiency, safety, long product lifecycles and system integration are more important than pure scaling at the smallest geometry.

Against this background, EU semiconductor value-chain revenues have increased almost steadily, from EUR 53 billion in 2019 to an estimated EUR 93 billion in 2025, as shown in the figure below which displays the EU's semiconductor value chain market in absolute values and the EU's share from 2019 to 2030. This growth is expected to continue, almost linearly, to EUR 143 billion in 2030.

In 2025 the EU's share of global value chain revenues is estimated at 8.8%, still far from the 20% target to be reached by 2030. This share is projected to remain relatively stable in the coming years, in a context of sustained large-scale investments in other regions of continued expansion in the global market which is now projected to exceed EUR 1.6 trillion in 2030. The EU market continues to grow in absolute terms. Although the EU share values are not increasing, the value of the EU27 semiconductor market has increased by 9.4% since 2024, compared with 8.0% growth in global market revenues (Figure1). EU semiconductor value-chain revenues have also increased by 4.5%, from 89 in 2023 to 93 billion euro in 2025.

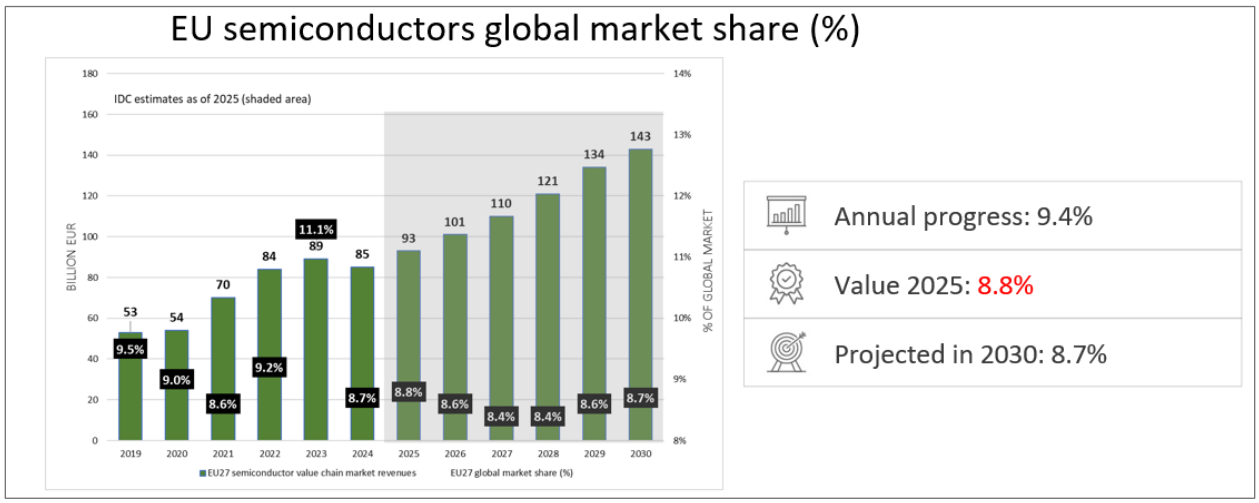


Figure 1: EU semiconductors value chain revenues (on the left axis in billion EUR) and global market share (on the right axis in %). The EU market shares are shown in the black labels (Data source: International Data Corporation)[4].

In their National Roadmaps, in 2025 Member States committed to investing EUR 50.2 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. The 53 measures reported in the roadmaps mainly focus on supporting R&D and on boosting production capacity and industrial deployment of semiconductors. Roughly one-third of the measures are dedicated to each of these areas, pointing to a balanced approach to growth and innovation. These areas also remain a priority in the Member States' roadmap adjustments.

The European Chips Act[5] has established a framework to attract investments from semiconductor manufacturers into first-of-a-kind EU facilities. Since the launch of the initiative, already 13 projects have been announced representing more than EUR 32 billion in investments, with other promising projects upcoming. The Important Project of Common European Interest on Microelectronics and Communication Technologies (IPCEI ME-CT) is now fully operational. It brings together 14 Member States and 47 companies, channelling around EUR 20 billion from both private and public sources into 57 collaborative projects across several countries, out of the 68 projects initially envisaged (due to some withdrawals or early conclusion). In parallel, the proposed new IPCEI on Advanced Semiconductor Technologies (IPCEI AST) is expected to enter the notification phase shortly.

The Chips Act, through the Chips for Europe Initiative, has also launched a set of initiatives aimed at building technological capacity and accelerating the transfer of innovation from research to industrial

[4] Updated foreign exchange calculations can retroactively change historical data. While base market figures remain the same, their currency conversion and normalisation are adjusted every year.

[5] Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act)

deployment. State-of-the-art pilot lines, supported by a total of EUR 3.7 billion funding, offer shared, industrial-scale environments where new technologies can be tested, validated and prepared for production in key areas such as beyond 2nm leading-edge system-on-chip, fully depleted silicon-on-insulator applications, advanced packaging, wide-bandgap materials, and photonic integrated circuits. The design platform focuses on reinforcing the EU's capabilities in chip design, enabling companies (particularly SMEs and start-ups) to develop more complex and system-level products. Competence centres serve as entry points to expertise, training and technology support, anchoring knowledge in regional ecosystems, and facilitating access to infrastructure and skills across Member States. Competence centres may also support regions within each Member State in developing long-term strategy to host, attract and expand semiconductor-related investments to the benefit of the local ecosystems. Quantum chip pilots prepare Europe for emerging computing and sensing technologies by creating pathways from frontier research to manufacturable components, while the Chips Fund complements these infrastructures by improving access to risk finance and scale-up capital.

For the European Union to compete globally in the semiconductor sector, it is essential that each Member State develops national semiconductor strategy providing strategic objectives, priorities and relevant roadmaps, to substantially increase investments and to continue 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 has started the formal review of the Chips Act, targeting the Chips Act 2.0 announcement in Q2 2026 with a clear support from industry, and Member States.

Public funding must also strike the right balance between predictability and flexibility, while crowding in the much-needed private investment and avoiding distortions of competition in the internal market. A stable and predictable trajectory is essential for budget planning, but the pace of technological development also requires the capacity to respond swiftly to emerging priorities. In this respect, Joint Undertakings (JUs) are comparatively well equipped, as their procedures allow work programmes to adapt more rapidly when new needs arise. By pooling public and private resources at scale, JUs have played a pivotal role in aligning strategic agendas, and fostering robust ecosystems around key EU policy priorities, thereby strengthening Europe's competitiveness and technological sovereignty. However, Member States' financial planning has not always been sufficiently flexible to accommodate emerging needs and changing priorities. In addition, due to the complexity of rules applicable to the blending of funding, Member States' departments responsible for R&I funding in JUs must ensure close coordination with state aid experts, a process that can lengthen administrative timelines before final decision making.

Recommendation:

Member States should accelerate the development of the EU semiconductor value chain, in line with the Chips Act and in view of the forthcoming Chips Act 2.0, by:

(i) developing semiconductor strategies and inserting relevant policy measures in their National Roadmaps reflecting their contributions towards the objectives and provisions of the proposed Chips Act 2.0;
(ii) stimulating their national fabless ecosystem by promoting start-ups and scale-ups and investing in design centres;
(iii) strengthening the ability of companies in their territory to develop, integrate, and use semiconductor technologies, by promoting competence centres and skills development;
(iv) identifying and supporting European regions that demonstrate a credible long-term strategy to host, attract and expand semiconductor-related investments;
(v) streamline permitting procedures and reduce time for granting permits for semiconductor facilities; and
(vi) mobilize national and regional investment to support relevant semiconductor initiatives.

Member States participating in the Chips Joint Undertaking should:
(i) ensure predictable and rapid national co-funding for projects under the Chips Joint Undertaking, including pre-allocation of dedicated national budgets, automatic match-funding mechanisms for selected proposals, and simplified national approval procedures;
(ii) anticipate national budget planning to accommodate multi-annual work programmes and several call launch dates within a single calendar year;
(iii) reinforce State aid expertise in national administrations responsible for R&I funding, in coordination with national representatives in the Chips Joint Undertaking.

2.1.2 Quantum

The starting value for this KPI was 0 in 2022 and it reached and surpassed the target in 2024 as the first two quantum simulators were deployed in France and Germany, see trajectory (Figure 2). Additional quantum computers are expected to be deployed before the end of the decade, as several procurements are currently ongoing. Given the specific nature of this target, no baseline trajectory has been established.

In their National Roadmaps, Member States reported investing EUR 4.1 billion in quantum computing (1.4% of the total budget of the National Roadmaps), of which EUR 358 million comes from private sources. The 62 measures reported mainly focus on supporting R&D and the deployment of 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.

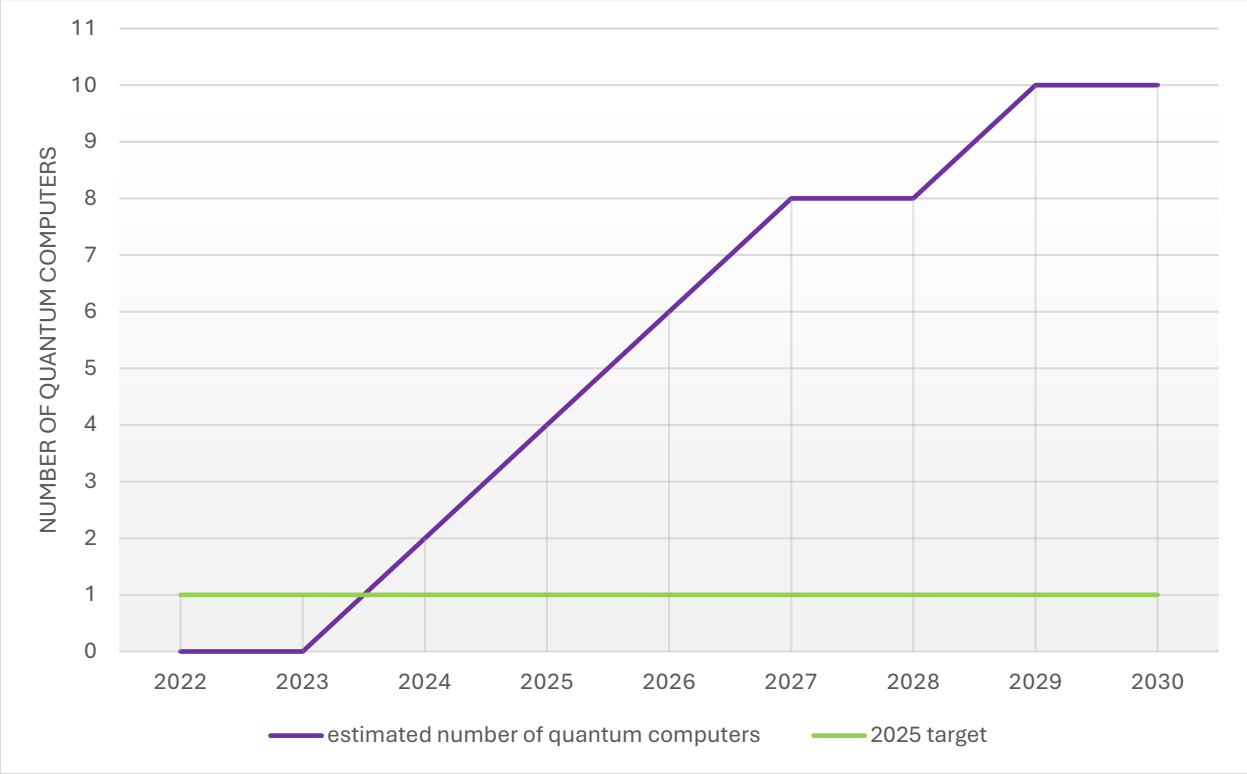


Figure 2: Number of quantum computers in the EU. Trajectory towards 2030.

The target for the Quantum KPI has been reached and the KPI has currently a value of 6, expecting to reach 10 by the end of the decade.

The main challenge for the EU in this area remains fragmentation. Globally, in 2025, it is estimated that there were more than 100 quantum computers[6]. Europe overall hosts around 40% of these systems distributed across more than 20 vendors. However, all these systems are **Noisy intermediate-scale quantum (NISQ**) systems with a low number of qubits (< 1000) and error rates that do not allow computations demonstrating a clear quantum advantage.

For the EU to lead in this field, Member States need to coordinate their efforts and investments to support the scaling up of the technology. Building a fault-tolerant quantum computer (FTQC), will require a very substantial investment by the EU and the MSs (hundreds of millions EUR[7]), together with private and venture capital. Such a computer, operating with stable logical qubits, will be capable of running algorithms that demonstrate a quantum advantage.

[6] Donovan, Quantum computers: 100+ Estimated by 2025, March 2025.

[7] Bao Tran, How Expensive Is It to Run a Quantum System? (Stats Inside), April 2026.

Progress towards this stage will therefore depend on joint cooperation and sustained investment focused on carefully selected technological priorities. Other countries, notably the United States have launched such initiatives[8] including ones that are also open to foreign companies. If the EU does not act in time, there is a risk that European companies will develop and commercialise their technologies outside the Union or be acquired by foreign competitors, with the related technology and intellectual property subsequently developed outside the EU.

The recently published Quantum Europe Strategy[9] sets out the objectives in this area while the upcoming Quantum Act will provide the legal and budgetary framework for reaching them.

Finally, Europe also needs to increase its share of private investment in quantum technologies. While the EU still leads in terms of the number of investments, in 2025, out of the USD 4.36 billion invested globally in quantum technologies, companies in Europe attracted only 23% of the global amount invested (USD 1.014 billion), compared to 64% attracted by companies based in the United States[10]. Moreover, these private investments in the EU represent only 10% of the total public investments (MS and the EU combined)[11].

In the domain of quantum communications, the global leader is China with rapidly expanding ground optical quantum networks as well as multiple quantum communication satellites. The EuroQCI[12] initiative aiming at deploying a secure quantum communication infrastructure across Europe is an ambitious European response, encompassed in the IRIS^2 Secure Connectivity regulation.

Recommendation:

Member States should strengthen their investments and support in quantum technologies, in line with the Quantum Europe Strategy and the forthcoming Quantum Act, by:

(i) aligning and coordinating national quantum strategies and Roadmaps with the EU quantum roadmap

(ii) supporting the scale-up and deployment of critical quantum infrastructures, such as quantum computers and simulators, quantum chip pilot lines and design facilities, EuroQCI terrestrial and space secure communication networks, quantum internet testbeds and quantum sensing/PNT (positioning, navigation and timing) capabilities;

(iii) strengthening the quantum ecosystem, by supporting the further development of national and regional competence centres, promoting innovation procurement in favour of start-ups, scale-

[8] DARPA, QBI: Quantum Benchmarking Initiative, March 2026.

[9] European Commission, Quantum Europe Strategy, July 2025.

[10] Zenodo, Quantum Technologies Investment Report 2025, March 2026.

[11] JRC Publications, Future Directions for Quantum Technology in Europe, October 2025

12 European Quantum Communication Infrastructure - EuroQCI | Shaping Europe's digital future

ups, adopting public-sector first buyer measures, and fostering standards, benchmarking, and trusted quantum supply chains and

(iv) developing the corresponding talent pool in quantum in coordination with the future European Quantum Skills Academy.

2.1.3 High-performance computing, AI Factories and AI Gigafactories

Since its establishment in 2018, the EuroHPC Joint Undertaking (EuroHPC) has built one of the most powerful infrastructures for high-performance computing (HPC) and artificial Intelligence (AI) worldwide. Together with its participating states, the EuroHPC has acquired nine supercomputers, including three systems-JUPITER (#4), LUMI (#9), and LEONARDO (#10)-ranked among the ten most powerful supercomputers in the world. In September 2025, JUPITER, the first European supercomputer to reach the exascale frontier, was inaugurated. A second exascale supercomputer (Alice Recoque) is to be deployed within 2027. Several additional mid-range EuroHPC systems are currently being installed. These efforts have contributed to the development of a world-leading, secure, and interconnected supercomputing ecosystem, broadening HPC use, and strengthened the skills base for European science and industry.

The EuroHPC Joint Undertaking is rolling out 19 AI Factories and 13 Antennas across Europe, with an overall investment of around EUR 2.6 billion. This involves the procurement of 15 new AI-optimised supercomputers, increasing Europe's AI computing power fivefold. AI Factories and Antennas will cooperate as a federated network ensuring seamless integration, efficient resource sharing, and secure cross-border access, thereby advancing Europe's strategic autonomy in critical digital capabilities.

A major scientific success story of 2025 was the advancement of the Destination Earth initiative, which performed frontier high resolution climate simulations primarily using the LUMI supercomputer and its new AI Factory capabilities.

Europe stands at a pivotal moment to convert recent progress in HPC and AI into durable leadership, technological sovereignty, and broad-based impact. Expanding AI computing capacity within the EU remains a top-tier strategic priority to strengthen competitiveness and technological sovereignty. Building on the concept of AI Factories, AI Gigafactories are intended to take this a step further by integrating massive computing power in large-scale facilities designed to develop, train, and deploy the next generation of the most complex AI models at an unprecedented scale.

AI Gigafactories will be selected through an official Call, based on joint procurement between EuroHPC and its participating states. These infrastructures are essential if Europe is to compete at the global level and strengthen its strategic autonomy in science and in critical industrial sectors. Given the scale of investment required, AI Gigafactories are expected to be implemented through public-private partnerships.

A critical factor in the HPC/AI ecosystem remains the strong dependence on third-party sources, notably for HPC and AI chips. For a sovereign ecosystem to thrive, the EU must develop indigenous building blocks (i.e., the necessary hardware and software) to power these supercomputing infrastructures. Europe has strong engineering talent in the field, but producing competitive European alternatives-spanning semiconductor design, packaging, integration, and optimised software stacks-will require sustained funding and industry partnerships well placed to bring these capabilities from prototype to volume deployment.

Recommendation:

Member States should reinforce their HPC and AI infrastructure investments to ensure that businesses, researchers and public administrations have access to the computing resources required for serving their AI developments and services, including the specific needs of model fine-tuning and inferencing, notably by:

(i) leveraging the network of AI Factories and Antennas fostering services –including Data Labs– which target the specific needs of their national AI developers and innovators;
(ii) supporting and promoting the development, deployment and operation of AI Gigafactories;
(iii) developing quantum-enhanced machine learning applications;
(iv) investing in EU-sourced HPC and AI hardware and software to attain strategic autonomy and guarantee public and industrial security;
(v) developing the corresponding talent pool in HPC and AI, in coordination with the EU Digital Skills Academies.

2.1.4 Edge nodes and computing capacity deployment

Edge computing is emerging as a critical complement to traditional cloud infrastructure. While the current wave of artificial intelligence-particularly generative AI-relies heavily on centralised, high-performance computing resources hosted in hyperscale cloud environments and High-Performance Computing (HPC) centres, an increasing share of data processing is shifting closer to where data is generated. Edge nodes enable low-latency processing, real-time analytics, and more efficient data handling by reducing the need to transmit large volumes of data to distant cloud facilities. In this architecture, cloud and edge operate in tandem: the cloud provides the large-scale computational power required for training and orchestrating AI models, while edge infrastructure supports inference and time-sensitive applications at or near the end user. Beyond incremental optimisation, there is also an evolution towards “native AI,” which requires embedding AI directly into system design rather than layering it onto existing architectures. Although more complex, this approach unlocks significantly greater performance gains-much like 5G standalone delivers far higher capabilities than non-standalone 5G despite sharing the same label.

In 2025 the Edge Observatory methodology has been significantly improved based on the lessons learnt in the previous years of the analysis. The updated methodology is based on a Computer-Assisted

Telephone Interviewing - CATI - survey of more than 430 validated respondents across all the EU Member States. The respondents are selected amongst IT infrastructure decision-makers surveyed in their local language. The stratified sample is selected according to geographical distribution, type of industry (according to Eurostat's official classifications NACE Rev. 2), and company size. The platform *DataCentreMap*[13] is used to monitor public edge nodes. On-premise node figures, limited to enterprises with 250+ employees, are derived on the basis of Eurostat's enterprise statistics combined with site-to-node ratios by the Germany's Federal Statistical Office, used as a proxy in the absence of equivalent EU-wide data. A series of validation interviews with both CATI respondents and external experts are carried out to cross-check the results, supported by multi-source triangulation and outlier disqualification to ensure statistical robustness. For these reasons, 2025 data cannot be compared with previous years (break-in-series)[14].

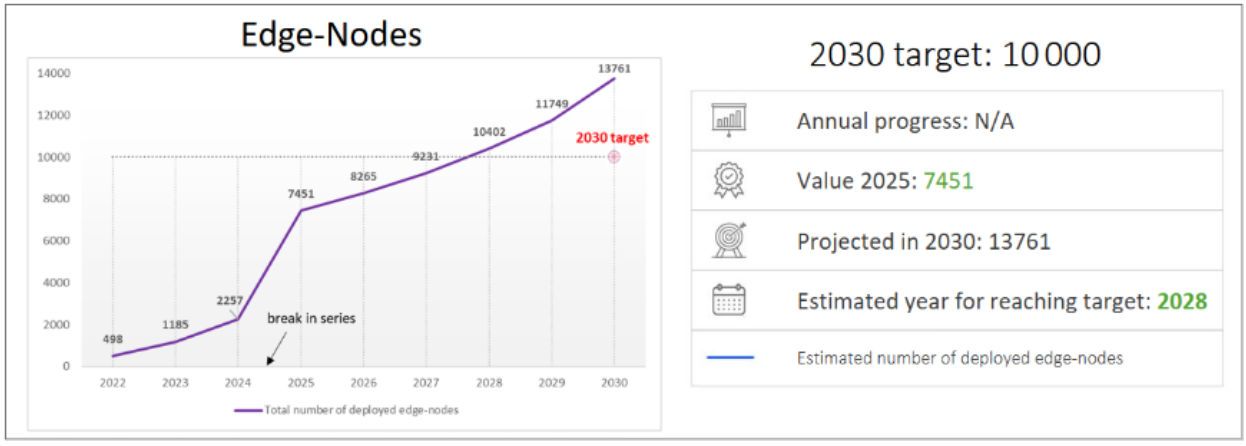


Figure 3: Edge node estimated deployment (EU projection to 2030).

As of end-2025, the Edge Observatory for the Digital Decade estimates that 7 451 climate-neutral and highly secure edge nodes[15] are deployed across EU, spanning four categories: on-premise, far edge, near edge, and in-country edge data centres. Private on-premise near edge (295 nodes), and far edge (67 nodes).

Despite representing only 6% of nodes in 2025, in-country data centres account for the large majority of total edge capacity - potentially up to 92% of aggregate MW if nodes operate at maximum rated capacity.

[13] Data Centre Map website, search tool, https://www.datacentermap.com/.

[14] Edge Observatory for the Digital Decade, D3 – Edge Nodes Taxonomy and Monitoring Methodology 2024; D4 – Edge Nodes Deployment Progress Report; D6 – Edge Nodes Deployment Progress Report.

[15] A climate-neutral and highly secure edge node is a compute node designed and operated to achieve net-zero carbon impact while ensuring both physical and cyber security for uninterrupted operation and data safety. See Edge Observatory for the Digital Decade Edge nodes taxonomy definitions in Edge Observatory for the Digital Decade – Edge Computing for full detail.

On-premise nodes, by contrast, despite constituting 89% of all nodes, represent a comparatively modest share of total capacity, given the small footprint of each individual deployment (approximately half a rack).

When sustainability and security criteria are set aside, the total on-premise edge population alone exceeds 17,000 nodes, indicating a large share of deployments that do not yet meet climate-neutral and security standards.

Edge node deployment across the EU27 remains heavily concentrated in larger, high-GDP economies, with Germany leading both on-premise and public edge deployments. In 2025, Germany leads with 1 771 carbon-neutral and secure on-premise edge nodes, followed by France (737), Italy (629), Poland (536), and Spain (529). For public edge nodes, Germany, France, and the Netherlands together account for 51% of all public edge nodes in the EU27, with regional hotspots in West-Nederland (Amsterdam), Hessen and Nordrhein-Westfalen (Frankfurt area), and Île-de-France (Paris), all areas with established colocation and hyperscale data centre infrastructure. Deployments strongly favour metropolitan and industrial zones, while rural areas and transport hubs remain the lowest priorities. Future expansion is expected to broaden geographic and service zone coverage, although targeted rural deployment remains the least anticipated growth dimension.

The total number of climate-neutral and highly secure edge nodes deployed across EU27 Member States is projected to reach approximately 14 000 by 2030, representing an 88% increase relative to the estimated 7 451 nodes deployed at end-2025[16]. On this basis, **the Digital Decade target of 10 000 nodes is projected to be reached in 2028, two years ahead of the 2030** deadline.

It is expected that on-premise nodes will retain structural dominance throughout the period, although their relative share is forecasted to decline modestly from 89% to approximately 84% as near edge infrastructure scales more rapidly. Public edge infrastructure (in-country data centres, near edge, and far edge combined) is projected to more than triple from around 1,032 nodes in 2025 to over 3 500 nodes by 2030. This is expected to translate into a significant expansion of aggregate compute capacity at the edge by 2030.

The expansion of edge nodes must be analysed and contextualised within the broader context of cloud infrastructure, which continues to underpin the overall availability of **computing capacity**. The rapid advancement of AI is fuelling an unprecedented surge in demand for **computing power**[17]; not only for edge nodes needed to low-latency solutions, but also for the broader **computing capacity**, i.e. the total

[16] Edge observatory for the Digital Decade (Consortium analysis and projections based on CATI survey and DataCentreMap, December 2025.

[17] CSET Issue Brief, AI and Compute: How Much Longer Can Computing Power?, January 2022.
McKinsey Quarterly, The cost of compute: A $7 trillion race to scale data centers, April 2025.
Bain & Company, How Can We Meet AI's Insatiable Demand for Compute Power?, September 2025.
Goldman Sachs AI to drive 165% increase in data center power demand by 2030, February 2025.
HAI Stanford, The 2025 AI Index Report, 2025.

volume of processing resources available, required to support fine-tuning of models and inference. Beyond AI, the adoption of cloud computing and other digital services continues to accelerate, further intensifying the pressure on available infrastructure. In this regard, the current investigations opened under the Digital Markets Act[18] in relation to the cloud computing sector are exploring the need and possibility to unlock opportunities and support fairness and contestability in the provision of cloud services. In addition, interested Member States are designing an Important Project of Common European Interest (IPCEI) focusing on the deployment of a Compute Infrastructure Continuum (CIC), namely a distributed and federated network of digital infrastructure, aiming to further increase compute capacity availability in Europe and enable functionalities, including but not limited to AI. In 2025, per Eurostat, EU business cloud uptake stood at 46.7% - still far from the 2030 target of 75%. As more European businesses adopt cloud and AI computing services, demand for data centres is therefore expected to rise further. In 2025, the EU's computing capacity was estimated at approximately 12 GW[19].

The EU continues to lag behind other regions in both the scale and ownership of digital infrastructure[20]. Despite comparable GDP levels, the EU accounted for only 20% of global data centre capacity in 2025, while the US held 42%. Although this capacity is expected to grow in the coming years, the gap relative to projected needs is also expected to widen. Market evidence points to tightening conditions for capacity expansion, with demand for colocation space in Europe exceeding new supply despite investments[21]. In 2025, demand for new data centre capacity in Europe reached a record of 854 MW, outstripping new supply for the third consecutive year. Across EU-27, the expansion of data centre capacity is therefore not able to keep up the pace with the rapidly growing demand[22]. Since 2022, average asking prices in European colocation markets have surged by 51% for 100 kW leases.

While cloud and AI computing services can be technically delivered cross-border, regions with a low data centre presence are disadvantaged by the existing geographic imbalance in infrastructure deployment, as reflected in higher prices in regions with low data centre capacity[23]. Moreover, the lack of nearby computing capacity drives up latency, limiting the availability and quality of low-latency services, thus placing local end-users at a competitive disadvantage compared with regions that have better access to

[18] European Commission, Commission launches market investigations on cloud computing services under the Digital Markets Act, 18 November 2025.

[19] Data centre capacity is typically expressed in megawatts (MW) or gigawatts (GW) because power availability plays a key role for both the operation of the servers and the cooling systems. The estimated capacity is based on the Technopolis Group, Wavestone, Timelex, STL Partners, OpenForum Europe and KAPA Research (2025), "Study: Cloud and AI". The methodology is based on all known commercial data centre sites listed in the *Data Center Map*, additional sites identified through the survey and any publicly known hyperscalers sites. The figures do not include private enterprise sites.

[20] Groupes D'Etudes Géopolitiques, International comparisons and the state of AI infrastructure strategies, February 2025.

[21] Data Centres | CBRE, Rents will continue to increase, January 2025.

[22] Savils, Costs on the rise, May 2024.

[23] ServerMania, Cloud Server Pricing Guide: Transparent Costs & Comparisons for 2026, January 2026.

DC capacity[24]. Some of the identified key bottlenecks slowing down the deployment of computing capacity across the EU include regulatory fragmentation, permitting procedures, limited land availability, and increasingly, constraints of energy supply. The current regulatory environment remains fragmented, with different rules and permit requirements across Member States, creating uncertainty and delays for data centre operators. Permitting procedures are often lengthy and inconsistent, with multiple stakeholders and decentralised decision-making. Additionally, access to suitable land, affordable energy, and grid capacity is a significant challenge, particularly as energy prices in Europe are significantly higher than in other regions[25].

Insufficient computing capacity in the EU could slow innovation and the diffusion of cloud and AI services, increase dependence on non-EU providers, and limit the ability of businesses and public services to meet growing demand for digital services. There is no direct quantification of the consequent direct impact on innovation, but literature suggests that AI adoption can generate significant gains in productivity meaning that any capacity gap would risk delaying or displacing these gains. This impact would not only concern AI deployment but also digital services that are heavily reliant on cloud infrastructure. Stakeholders, including Mistral AI, have warned that insufficient data capacity would become a roadblock for developing and applying AI in Europe. Over time, persistent disparities risk slowing digital transformation in affected member states, widening gaps in terms of digital adoption and deployment and thus undermining the competitiveness of the Digital Single Market.

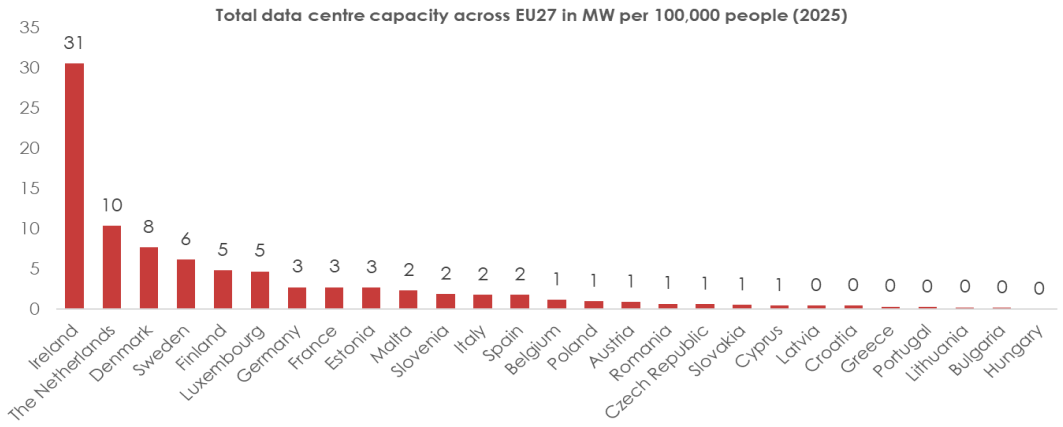
Against this background, the Commission's Cloud and AI Development Act aims to triple EU data centre capacity within the next years, with a focus on sustainable infrastructure. Looking ahead, regular monitoring of this capacity would be beneficial, yet a significant challenge will be ensuring consistent measurement throughout the EU, as differences in definitions, metrics and scope currently complicate precise comparisons.

[24] Taking the Azure network round-trip latency statistics (June 2026), round-trip latency (the time it takes for a data pack to travel from one point in the network to another and back again) from Poland (Central Europe) to Frankfurt (Western Europe) is ca. 10–15ms, and latency from Poland to Amsterdam or London is ca. 15–20ms. By contrast, latency within Western Europe (e.g. Frankfurt to Amsterdam) is typically <5ms. A fintech business in Warsaw thus faces significantly higher latency than a competitor in Western Europe.

[25] IDC, IDC Report Reveals AI-Driven Growth in Datacenter Energy Consumption, Predicts Surge in Datacenter Facility Spending Amid Rising Electricity Costs, 2024; See also: CERRE, From Gridlock to Grid Asset: Data Centres for Digital Sovereignty, Energy Resilience, and Competitiveness, September 2025, pp. 13–15.

Focus box: Member States' computing capacity deployment – first monitoring exercise

This first data centre monitoring exercise compares Member States' estimated data centre capacity using data centre capacity per 100 000 people. The EU benchmark used is the **EU average excluding Ireland**, because the country is a clear per capita outlier. On this basis, the **benchmark is 2.43 MW per 100 000 people**[26]. This evidence on data centre capacity comes from the results of the Cloud and AI Study for the Impact Assessment preceding the Cloud and AI Development Act[27]. The study collected information on colocation and hyperscale datacentre facilities both in cloud and edge installations. It did not cover enterprise data centres, including in-house facilities operated directly by companies or public administrations for their own use[28].



Ireland's position reflects the very high concentration of hyperscale infrastructure hosted in the country, linked to its role as a European base for major technology companies, as well as its strong transatlantic connectivity and attractiveness for foreign direct investment in digital services[29].

The Netherlands also stands out from the rest of the EU27, once Ireland is treated separately as an outlier, with a very high data centre capacity per 100 000 people. This suggests a highly developed data centre market and a very strong domestic infrastructure base. Denmark, Sweden, Finland and Luxembourg also perform well above the EU average in per capita terms and have relatively strong domestic capacity bases. The remaining challenge for these countries focuses therefore mainly on

[26] Population figures are based on Eurostat 2025 population data; Eurostat estimates the EU population at 450.4 million inhabitants on 1 January 2025.

[27] Technopolis et al. (2025), "Study: Cloud and AI". The study figures are presented in the Impact Assessment for the Cloud and AI Development Act: https://ec.europa.eu/newsroom/dae/redirection/document/129113

[28] As a result, the figures should be interpreted as an estimate of the commercial and hyperscale data centre capacity captured by the monitoring exercise, rather than a complete inventory of all data processing infrastructure in each Member State. This scope limitation is particularly relevant for Member States where a larger share of capacity may be hosted in enterprise or public sector facilities. Moreover, the chart shows data centre capacity in operation or planned for the near future and thus may not capture major projects under construction or announced investments (e.g. Greece's Microsoft's Attica data centre, or Portugal's Sines data centre campus). While the results should thus be interpreted with caution, they still provide a useful basis for identifying potential capacity gaps and policy needs.

[29] Why So Many Data Centres Are Being Built In Ireland?

sustainable management of further growth. Germany, France and Estonia appear close to, or slightly above, the EU average, suggesting continued pressure to keep pace with growing cloud, AI, public sector and industrial needs.

Malta, Slovenia, Italy and Spain fall below the EU per capita average, but their situations differ in scale and maturity. Spain and Italy already have significant absolute data centre capacity and growing markets, with remaining challenges around sustainability and uneven regional distribution. Slovenia and Malta have smaller domestic markets and could benefit from ensuring sufficient and resilient capacity for critical public services and strategic workloads.

Belgium, Poland, Austria, Romania and the Czech Republic, also appear below the EU average despite having strategic geographic or economic advantages. Key challenges include leveraging existing connectivity infrastructure into domestic capacity, keeping pace with cloud, AI and cybersecurity demand, and navigating constraints such as grid access, permitting and coordination. Slovakia, Cyprus, Latvia and Croatia have relatively small domestic capacity bases, raising questions about resilience, business continuity and strategic autonomy. Given their small market size, the challenge for these countries centres on establishing a minimum secure and reliable domestic capacity base for more critical workloads.

Greece, Portugal and Lithuania show very low current capacity in the monitoring exercise and could benefit from converting strategic geographic positions and submarine cable connectivity (notably Portugal's Atlantic links and Greece's eastern Mediterranean role) into domestic capacity and strategic autonomy. Bulgaria and Hungary appear among the weakest performers in the dataset, with Hungary recording the lowest capacity overall, reflecting possible limited market demand or infrastructure gaps. This could pose strategic autonomy risks as future needs grow for cloud adoption, AI readiness, public sector digitalisation and industrial data.

This monitoring exercise will be further structured and refined in the coming years as part of the implementation activities foreseen under the Cloud and AI Development Act.

Recommendations:

Member States should support the deployment of secure, sustainable and sovereign cloud and edge data centre infrastructure across the Union, in line with the principles of the proposed Cloud and AI Development Act, by:

(i) supporting the development and deployment of advanced data centre technologies that power edge and cloud computing infrastructures incorporating energy- and resource-efficiency principles by design and throughout operations with a view to achieve large-scale sustainability;

(ii) supporting the development and deployment of secure, resilient and performant open cloud and AI stack technologies able to operate cloud and edge computing infrastructures and services with a view to build European technological autonomy and safeguard the Union's digital sovereignty;

(iii) facilitating the deployment of AI compute infrastructure across Europe to close the capacity gap and meet the Union's needs;

(iv) engaging with the Commission, in the context of the upcoming review of the Digital Decade Policy Programme, on the establishment of a new target to monitor and benchmark edge, cloud and AI data centre infrastructure across Member States to measure needed capacity to prevent gaps, ensure balanced access, and build robust European AI capabilities.

Member States should develop **national cloud and AI strategies** (strategies). The strategies should address Member States approach to expanding cloud and data centre capacity as well as at advancing AI capabilities. Where Member States have identified gaps in possible existing strategies, Member States should update them accordingly. The strategies should be aligned with the targets on the adoption of cloud computing services, big data and AI by at least 75% of Union enterprises for their business operations, and the deployment of at least 10 000 climate-neutral highly secure edge nodes in the Union, while ensuring low latency. In that context, the measures adopted under the national strategies should inform the national digital decade strategic roadmaps.

Where Member States are deploying data centre capacity on their territory, they should designate d**ata centre acceleration zones** (zones). Within the zones, the development, expansion and modernisation of data centres may be facilitated through coordinated planning and streamlined administrative procedures. The designation of such zones should contribute to closing the capacity gap and improving the Union's competitiveness and technological resilience, while ensuring compliance with applicable Union law, including requirements relating to energy efficiency and environmental protection.

Member States should carry out **risk assessments** to analyse public sector activities and their sensitivity with respect to sovereignty of cloud and AI services underpinning such activities. The risk assessments should help Member States to establish the degree of sovereignty required from cloud and AI services procured and used by entities entrusted with such activities. The Commission will provide guidance to assist Member States in carrying out their risk assessments.

Member States should consider participating in future initiatives aimed at **federating and interconnecting their cloud infrastructures with other Member States**, to offer cloud- and AI-enabled public services in an efficient, scalable and portable manner. Member States are also encouraged to define their public sector cloud and AI policies in a way that accounts for future frameworks allowing for such a public sector cloud federation to emerge.

2.2. Supporting innovative companies with digital tools and resilient network

2.2.1. Connectivity

Connectivity is a fundamental enabler of the EU's long-term competitiveness, determining how enterprises and public services can share data, innovate and deliver value. High-quality, secure cross-border connectivity enables companies to leverage cloud and AI services, scale up and collaborate in EU-

wide value chains. Strong connectivity also improves the Union's resilience and preparedness by ensuring continuity and flexible reconfiguration of business and public service operations, including critical ones, in the event of disruption.

According to the **Digital Decade Eurobarometer** 2026, 81% of Europeans consider it important for the EU to ensure access to high-speed internet for all EU citizens, while 83% of respondents think the EU should cooperate with Member States to build an independent European digital infrastructure (including broadband, 5G, cloud, semiconductors).

Modern connectivity is evolving from a combination of separate technologies - fixed, mobile, satellite networks or submarine cables - towards a more integrated ecosystem. To respond to the growing demand for critical, low-latency applications, such as connected and automated mobility (CAM) and human-machine interaction, increasing volumes of data[30] need to flow seamlessly across all these domains, so that disruptions in one domain do not undermine the performance and security of the system as a whole. Demands on cross border backbone connectivity are also increasing exponentially: currently, cables worldwide transmit over USD 10 trillion in financial transactions on a daily basis[31] and capacity needs are expected to increase with AI and cloud applications. This evolution requires a global approach, spanning satellite, terrestrial and subsea infrastructures as part of a unified, resilient, and globally optimised system. Full fibre coverage, accelerated deployment of stand-alone 5G as a stepping stone to the development of 6G, and sufficient multi-orbit satellite capacity are the foundations for this approach.

I**ncreasing attention is paid not only to coverage, but also to the security and resilience of networks, as well as to integrated connectivity systems, as means of ensuring redundant and reliable connectivity**. The Council conclusions of 6 June 2025[32] call for **a comprehensive approach to the development of a reliable and resilient network infrastructure**, including via network diversification, interoperability and further deepening of the Single Market. They also called on the Commission to assess the possibility of a coordinated initiative for planning and developing a reliable and resilient network of digital infrastructures and capacities, including backbone terrestrial, submarine and satellite networks, across the Union and with international partner countries, for example by using the Trans-European Networks framework.

In their **National Roadmaps**, submitted in 2025, Member States reported devoting a significant portion (approximately 28%) of their measures' total budget to gigabit fixed connectivity, amounting to EUR 80.9 billion (with EUR 56.6 billion coming from private sources). The 106 measures reported mainly focus on regulatory actions to facilitate network deployment, as well as financial support for non-viable and commercially unattractive areas and strategic infrastructure, including cross-border 5G corridors, submarine cables, and secure backbone networks. Around one third of the measures are dedicated to

[30] Statista, Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2023, with forecasts from 2024 to 2028, 2025.

[31] FSISAC, FS-ISAC Releases Critical Guidance on Subsea Cable Risks for Financial Firms, December 2024.

[32] European Council, Transport, Telecommunications and Energy Council Conclusions, June 2025.

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 6 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.

However, recent territorial analyses indicate that improvements in connectivity do not translate uniformly into digital performance across regions. While infrastructure gaps persist in rural and peripheral areas, new divides are increasingly driven by differences in digital capabilities, usage patterns and local socio-economic conditions[33].

Fixed access networks

The next five years will be characterised by a progressive shift from the current fixed access networks towards ubiquitous, full-fibre infrastructures (from fibre-to-the-premise to fibre-to-the-room), offering symmetrical multi-gigabit speeds, ultra-low latency, high reliability and much lower energy consumption. Fibre is increasingly viewed as a strategic, future-proof asset, capable of supporting data-intensive applications such as cloud and edge computing, AI, Augmented and virtual reality (AR/VR), remote healthcare, smart grids and cities, and industrial automation. The growing need for symmetrical capacity will require significant infrastructural upgrades towards large scale multi-gigabit architectures.

Despite these increasing stakes, **the current pace of evolution in FTTH rollout remains insufficient.**

The percentage of households with fibre connection rose by 4.9 percentage points, from 69.2% in 2024 to 74.1% in 2025, representing a **year-on-year increase of 7.1%**. According to the forecast along the baseline trajectory, **90.1% of the target is expected to be achieved by 2030** (Figure 4). **In 2025, the FTTP coverage stood at about 80% of the ideal value along the digital decade trajectory** (74.1% instead of 94.0%). The full target - 100% of households covered - is forecast to be reached only in **2050** if no further actions are taken. **Only 62.7% of households living in rural areas were reached by fibre in 2025, up from 58.8% in 2024 (+6.7%).**

[33] ESPON, DigiReg – Territorial Perspectives of Digital Transition in European Regions, 2024.

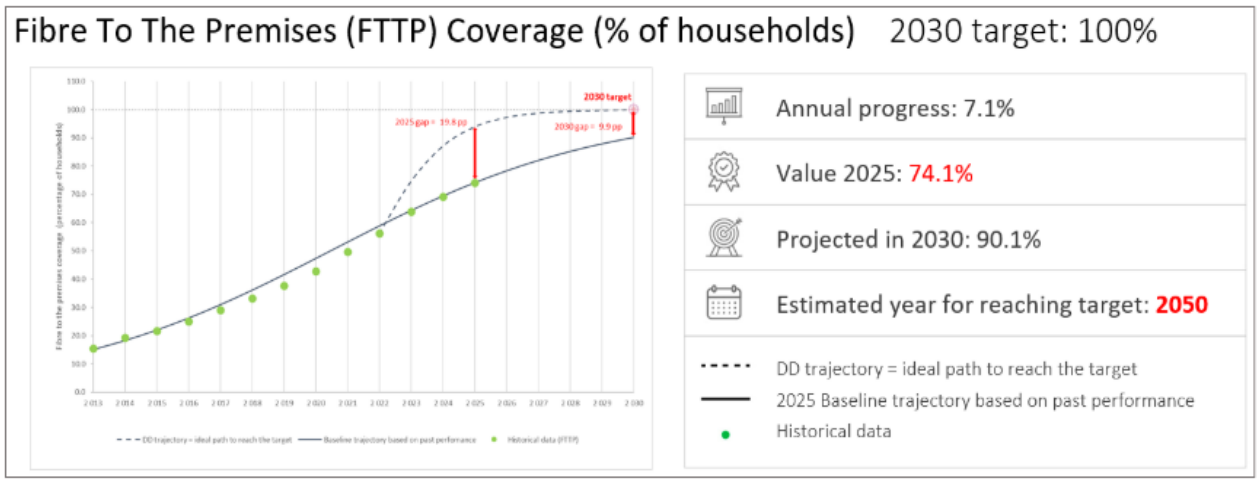


Figure 4: FTTP coverage in the EU. Historical data, Digital Decade (DD) trajectory and revised baseline trajectory towards 2030.

Take-up rates for high-speed fibre (FTTH) also **vary significantly across Member States,** remaining below 30% in some of them. Low adoption rates have reduced operators' returns on investment, particularly for smaller fibre providers without an established customer base, consequently reducing incentives for further investments.

To accelerate the transition from copper to fibre, the Digital Networks Act proposal[34] sets **an EU-wide copper switch-off objective for 2035**. This would however be subject to strict conditions on fibre coverage (95%) and availability of comparable retail offers. The proposal is also accompanied by several safeguards and supporting regulatory measures, regarding, in particular, the deployment of the last part of the fibre network connecting the end-user.

The investment needed to achieve 100% FTTP coverage - the Digital Decade target for 2030 - is estimated at EUR 40 billion, or EUR 29 billion if 5G Fixed Wireless Access (FWA) is used for remote areas. Therefore, **in order for the Digital Decade target to be achieved, it will be necessary to continue supporting fibre rollout, through the transition away from legacy copper networks.**

Mobile networks

In the coming five to ten years, **mobile networks** are expected to evolve from basic 5G to advanced 5G standalone (5G SA) and to 6G, delivering much higher capacity, ultra-low latency, and native support for AI-driven and immersive applications. They will become increasingly **software-defined, virtualised, and smart**, as AI is embedded in network management, optimisation, and security. Mobile networks will also be tightly integrated with fixed fibre networks to support dense small-cell deployments and with non-terrestrial networks to ensure ubiquitous connectivity. Beyond consumer connectivity, future mobile networks will increasingly serve **industrial, public-sector, and mission-critical use cases.** This will enable automation, smart infrastructure, and real-time services, with a **stronger focus on energy efficiency,**

[34] European Commission, The Digital Networks Act | Shaping Europe's digital future, January 2026.

resilience, and security as strategic requirements. **Mobile data usage per mobile connection in Western Europe is projected to rise to 49 Gb per month by 2030, compared to approximately 15.3 Gb per month in 2024[35].**

Convergence with fixed networks is expected to deepen, as fibre becomes essential for 5G SA/6G backhaul and fronthaul. Functional convergence with satellites is also progressing, with important implications for mobility and industry verticals and the connection of remote areas. 6G is expected to enable the seamless integration of terrestrial and non-terrestrial networks (NTNs), including satellite systems, into a unified architecture. This will support the scaling of direct-to-device (D2D) connectivity and enable ubiquitous, resilient and high-performance connectivity across both ground-based and space-based infrastructures. In this context, satellite connectivity is expected to become a native component of 6G networks, marking a shift from its traditional role in backhaul towards direct connectivity for end users.

Nevertheless, the EU's progress towards this transition remains very slow, not when it comes to basic 5G coverage, but with regard to the 5G networks able to deliver transformative services.

Member States are indeed very close to full basic 5G coverage (96.8% of households) with substantial coverage increases, including in rural areas; all EU Member States have basic 5G household coverage above 90%, except Romania. However, basic 5G coverage is insufficient, given its technological limitations, to support the EU goals in the area of competitiveness.

Mid-band deployment - which is associated with high-capacity, high reliability and low latency - remains a bottleneck. 5G mid-band coverage in the 3.4-3.8 GHz spectrum band is substantially lower than general 5G coverage in many Member States (74.8% overall household coverage). Rural mid-band coverage is particularly weak. The EU27 average of 5G rural household coverage in the 3.4-3.8 GHz band remains at around 33.8%, indicating that progress is largely confined to urban areas.

This gap is closely linked to delays and modalities in the assignment of all three 5G pioneer bands. The process of authorising 5G pioneer spectrum across the EU has been lengthy, fragmented and insufficiently predictable, spanning more than a decade. In particular, most national auctions for the 3.4-3.8 GHz took place over a relatively long period, between 2017 and 2024. Member States that assigned spectrum earlier reached higher population coverage more quickly than later movers[36].

This gap in high-capacity 5G deployment **limits the ability to deliver quality-assured services and advanced use cases**, such as industrial automation, connected mobility and other mission-critical applications, and **risks undermining Europe's competitiveness in next-generation digital services**.

[35] GSMA, The Mobile Economy Europe 2025, 2025.

[36] Commission Staff Working Document – Impact assessment report accompanying proposal for a Regulation on Digital Networks (Digital Networks Act).

Across Member States, 5G deployment remains predominantly based on Non-Standalone (NSA) architecture, which relies on existing 4G core[37]. **5G SA deployment (measured as 5G SA base stations as % of all mobile base stations) stands only at 20.9% in the EU,** below US (36.2%), China (34.8%), Japan (26.3%) and South Korea (26.2%)[38]. Other sources estimate that **only around 40% of the EU territory is covered by high capacity 5G SA**, compared to 91% in North America and 45% in Asia-Pacific, highlighting once again a significant infrastructure gap.

Most EU countries launched NSA networks between 2019 and 2021, enabling early market rollout. However, the transition to 5G SA, which introduces a fully virtualised 5G core and enables advanced capabilities such as network slicing, ultra-low latency, and 5G SA private network services, i.e. capabilities that are important for competitiveness of EU industry, has been more gradual and uneven in the EU than in other advanced economies.

Europe is also significantly lagging behind in take-up as in "basic" 5G take-up (measured as a share of 5G SIM cards among all SIM cards), the EU stands at (28.1%), which again places the region behind the leading developed countries. The US (56.7%), Japan (54.7%), South Korea (41.0%) and China (39.6% all have higher rates[39]. As of Q4 2025, only around 2.8% of 5G users in Europe are connected via SA networks, compared with approximately 30% in the United States, and far behind India and China, which have reached around 52% and 81% respectively[40].

The slow rollout of mid-band 5G, combined with the low pace of 5G SA adoption in Europe has direct repercussions for user experience. The EU27 average download speed of 69.9 Mbps remains below that of South Korea (162.2 Mbps), the US (129.3 Mbps), and China (100 Mbps)[41]. **This performance gap is economically significant, as empirical evidence shows that improvements in mobile broadband capabilities - particularly speed - are associated with higher productivity and GDP[42]**. Supporting evidence suggests that a 10% increase in mobile broadband speed is associated with a 0.2% increase in labour

[37] Connect Europe (2025), State of Digital Communication

[38] European Commission, European 5G Observatory 2026, 2026 (based on 2025 data published by operators and regulators, verified through interviews and complemented by IDATE estimates, as needed).

[39] European Commission, European 5G Observatory 2026, 2026.

[40] Ookla/Omdia, A Global Evaluation of Europe's Digital Competitiveness in 5G SA, February 2025; updated figures from Ookla, 5G SA Global Tracking, Q4 2025, February 2026.

[41] MedUX, Status of 5G Quality and Experience in Europe, Report prepared for the European Commission, Q1 2025.

[42] Briglauer, Wolfgang; Cambini, Carlo; Gugler, Klaus, Sabatino, Lorien (2025): Economic benefits of new broadband network coverage and service adoption: evidence from OECD member states, Industrial and Corporate Change, January 2025. See also: Edquist, H., "The Economic Impact of Mobile Broadband Speed," 23rd Biennial Conference of the International Telecommunications Society (ITS), June 2021; and Oxford Economics, The Global Economic Potential of 5G-Enabled Technology, March 2023.

productivity in the subsequent period[43]. In this context, Europe's comparatively weaker 5G performance may limit the realisation of potential productivity and economic growth gains.

In addition, **the EU trails other regions in the deployment of private networks**, which are early (industrial) adopters of 5G SA. Globally, 1489 private mobile network deployments have been identified, of which only 694 (47%) use 5G[44]. Manufacturing remains the leading sector for such networks, with 298 deployments recorded, of which around 60% include 5G. Asia-Pacific countries such as Japan and South Korea have progressed more rapidly, supported by more favourable policy frameworks and coordinated industrial strategies.

Relative to leading global markets, the EU remains less advanced in 5G investment intensity[45]. Its 51% 5G allocation share is solid (measured as % of all mobile investments), but below China (72%), South Korea (67%), the US (62%), and Japan (58%).

Achieving high-quality 5G SA coverage is estimated to require EUR 33.5 billion for network densification, with an additional EUR 26-79 billion needed to cover main transport paths[46]. The Digital Networks Act (DNA) proposal identifies disincentives and fragmentation in spectrum regulation as one of the main root causes of insufficient investments by European telecom operators in mobile networks. Other contributing factors include limited financial capacity and attractiveness for investors (itself due to low ARPUs, low predictability, etc.), low demand for advanced connectivity and unexploited economies of scale. For example, spectrum costs represent 7% of mobile service revenues and 35-40% of capital expenditure, reducing financial flexibility for 5G/6G investments. Additionally, fragmented and short-lived regulatory regimes act as disincentives.

A series of regulatory responses, essentially tackling the **supply side**, are offered in the DNA proposal, notably on spectrum policy. In particular, the DNA proposal simplifies and streamlines the regulatory framework that affects 5G and 6G rollout, with a view to reducing fragmentation across Member States and creating more predictable conditions. In doing so, it lays the groundwork for telecom innovation, particularly for emerging technologies such as 6G and satellite connectivity.

These proposed measures include unlimited spectrum licence duration by default and facilitated renewal procedures, affecting around 500 licences set to expire across Europe between 2025 and 2035, combined with safeguards such as periodic reviews, the possibility of revocation (e.g. in case of breach of conditions), and strong "use it or share it" obligations. They also include a pro-investment auction design, greater EU-level coordination through mandatory spectrum scrutiny and harmonised authorisation conditions (i.e. *ex-ante* Spectrum Single Market mechanism to ensure that auctions align with the objectives of the DNA)

[43] Edquist H. "The Economic Impact of Mobile Broadband Speed", 23rd Biennial Conference of the International Telecommunications Society (ITS), June 2021.

[44] Global Mobile Suppliers Association (GSA), Private Mobile Networks Summary Report, September 2024.

[45] European Commission, European 5G Observatory 2026, 2026.

[46] WIK-Consult, Investment and Funding Needs for the Digital Decade Connectivity Targets, 2023.

as well as faster and more predictable authorisation of future 6G spectrum to enable timely deployment. These measures are accompanied by other proposed measures on authorisation and governance, designed to facilitate larger scale operations and unlock the full potential of the single market.

The DNA also introduces a Union radio spectrum strategy to guide long-term spectrum planning, identify future needs, and ensure the availability of spectrum for key services and technologies.

It will, however, remain important to sustain public intervention in mobile access networks, including on **supply side** measures (i.e. public support to 5G/6G rollout) targeting areas of market failure in order to meet the Digital Decade targets, support cohesion and ensure that the Union's full industrial potential is fully exploited. Further actions remain necessary to support the ongoing implementation of the EU 5G Cybersecurity Toolbox and once adopted, to facilitate alignment with the trusted ICT supply chain security framework pursuant to the revised Cybersecurity Act.

Moreover, in order to address the root causes identified above, regulatory and funding measures may be complemented by **demand-side stimulation**, with a particular focus on enabling innovative business models, including the bundling of infrastructure deployment with edge cloud and AI integration and with concrete use cases.

Since 2021, the digital part of the **Connecting Europe Facility programme (CEF Digital) has co-funded 5G deployments integrated with edge-cloud computing and enabling innovative use cases** such as remote surgery, virtual reality for learning, drone-based monitoring and more. So far, a total of EUR 327 million were invested in 78 projects, including 47 projects for 5G Smart Communities and 31 projects for transport corridors. This funding has helped pave the way for the future development of vertical use cases for sectors considered as strategic for the economy.

In 2026, the Commission unveiled **EURO-3C, a EUR 75 million project meant to develop the EU's first large-scale federated Telco-Edge-Cloud infrastructure[47].** Financed via Horizon Europe, this landmark project, which brings together over 70 partners, will showcase the EU's ability to deliver cutting-edge digital services entirely through its own connectivity infrastructure, reducing reliance on third country providers. Telco-edge-cloud combines telecommunication networks, edge computing and cloud infrastructure into a single, integrated platform, bringing high speed, secure computing power closer to end-users.

EU's leadership in 6G will not be determined solely by leadership in radio technologies, but by its capacity across the converged digital communications stack, from advanced semiconductors to AI-driven network orchestration and cloud-edge integration.

[47] European Commission, Commission announces €75 million EURO-3C Project to build a federated Telco-Edge-Cloud infrastructure for digital sovereignty, March 2026.

The EU approaches the transition to 6G with a mix of structural strengths and growing dependencies[48]. It benefits from globally competitive vendors, strong radio access network (RAN) engineering capabilities, and recognised leadership in energy-efficient networks, supported by a coordinated research and standardisation framework, notably through the Smart Networks and Services Joint Undertaking (SNS JU) as well as large national 6G initiatives to promote European capacities in 6G and related technologies in a number of Member States (in particular Germany, Ireland, Spain, France, Italy, Netherlands, Finland, Sweden) [49] . These assets strengthen the EU's ability to influence global standards and ensure interoperability. However, challenges persist, including weaknesses in hyperscalers cloud services and AI development, reliance on external semiconductor supply chains, risks of diminished value capture in increasingly software-driven architectures, and exposure to geopolitical tensions and market fragmentation.

As value shifts toward cloud management software and AI orchestration, the EU risks losing ground in higher-margin segments if these capabilities remain externally dominated.

In conclusion, public investment - covering *inter alia* R&I, supply chain, network deployment, and fostering the take-up of advanced services - must continue to complement the new rules put in place with the proposed **Digital Network Act**, once adopted. Based on the lessons learnt from the current MFF, it will be essential to support 5G and 6G across the innovation journey, coupling network deployments with use cases and with the necessary edge, cloud and computing resources.

Satellite connectivity

Satellite systems provide broad regional and global coverage and, by their nature, can support a pan-European (or global) reach, unlike terrestrial mobile networks, which remain bounded by national deployment. As direct-to-device (D2D) connectivity is emerging, complementing terrestrial mobile services, as well as machine-to-machine services, including in underserved areas, the current EU framework - based on national authorisation regimes and national spectrum allocation - creates barriers to the provision of pan-European services. It also forces satellite operators to comply with divergent national rules and conditions across Member States in which they operate.

In particular, Low Earth Orbit (LEO) constellations supporting hybrid terrestrial-satellite systems or Non-Terrestrial Networks (NTN) are emerging as the modern equivalent of traditional mobile communication towers. They enable D2D connectivity and are expected to become an essential component of future 6G networks. Integration with terrestrial mobile networks (5G SA/6G) is expected to become central to future communications systems, enhancing resilience and ubiquity of connectivity. D2D satellite connectivity is rapidly emerging and may play a strategic role for mobile network operators (MNOs) and smartphone equipment manufacturers (OEMs). It presents a valuable opportunity to stand out in a saturated market,

[48] European Commission, European 5G Observatory 2026, 2026.

49 European Commission, European 5G Observatory 2026, 2026.

improve customer retention, and build long-term value. A global survey by Analysis[50], covering 18 500 respondents across 18 countries, highlights strong demand for D2D satellite messaging, showing that an early adoption of satellite D2D may be leveraged to attract and retain subscribers. Notably, 82% of subscribers considering switching providers within the next six months expressed interest in such services while 30% said they would be willing to pay for them.

Satellite infrastructure is also critical for ensuring equitable access to high-speed internet, especially in underserved and remote areas, while also strengthening the EU's capabilities in critical communications, including emergency and defence services. Although Europe was once a frontrunner in satellite communications, it has been slower to anticipate the innovation potential of this market and to invest in LEO constellation deployment and now lags behind the US and China. This increases the risk that the EU becomes dependent on non-EU providers of this critical infrastructure, with implications for both competitiveness and digital sovereignty, especially in a context of geostrategic uncertainty. According to a European Commission study[51] on Mobile Satellite Services in the 2 GHz band, as of March 2025 the EU has only 773 LEO satellites launched and 3 120 planned, compared with 220 launched and 27 198 planned in China and 7 633 launched and 33 397 planned in the US.

Looking ahead, the number of authorisations is expected to increase significantly, raising compliance costs for operators and enforcement costs for authorities. The coexistence of twenty-seven national authorisation regimes also contributes to coverage gaps and slows the rollout of pan-European satellite services.

The proposed DNA and MSS (Mobile Satellite Services)[52] Regulations introduce a single EU-level authorisation for satellite services ensuring EU-wide access to spectrum under harmonised conditions. This framework aims to create a level playing field, enable European operators to scale up, and support the development of innovative satellite services, such as D2D connectivity, which are increasingly critical for EU security and resilience. It also aims to strengthen the global competitiveness of EU operators and is expected to unlock further investment in satellite infrastructure. However, given the capital-intensive nature of satellite deployments and prolonged revenue realisation timelines, structured public-private partnerships, and strategic Union initiatives, remain key to accelerating this transformation and securing independent European infrastructure capabilities.

Backbone networks

The growing traffic in access networks, combined with rising data flow from and to edge, cloud, AI capacities and Content Delivery Networks, will require massive scaling of **backbone networks**. This will rely on advanced optical technologies such as coherent transmission, higher-order modulation, and open line systems, enabling **multi-terabit capacities** per fibre. Backbone networks will increasingly interconnect

[50] Analysys Mason, MNOs and OEMs need to adapt D2D now, June 2025.

[51] Detecon International GmbH, Study on Mobile Satellite Services (MSS) in the 2 GHz Band in the EU – Implementation of the Current Regulatory Framework and an Overview of the Satellite Connectivity Market, European Commission, 2025.

[52] COM(2026) 311 final

distributed data centres and edge nodes, reduce latency and support real-time and mission-critical services.

Backbone architectures will also become more **software-defined and automated**, as **resilience, security, and redundancy** become increasingly strategic priorities. This includes route diversification, protection against physical and cyber threats, and greater focus on submarine and cross-border terrestrial links as well as related deployment, maintenance and repair capacities (e.g. multi-purpose, modular vessels). The migration process to Post Quantum Cryptography shall safeguard the continuity of services, availability of data, and use of applications, and require coordinated action also across different types of networks, given the many interdependencies and interfaces. Quantum communications technologies will be integrated into critical backbone networks to support highly secured, mission-critical applications (e.g. QKD between Member States or banking companies).

The rollout of future backbone networks will not only be driven by cross-border and intercontinental connectivity needs but also by the deployment of data centres and computing capacities in **geostrategic and areas where renewable energy is abundant,** located close to clean power sources (e.g. solar or hydropower plants).

In particular, the total value of **submarine communication cables' global sales was estimated at USD 3.8 bn in 2024** and is expected to reach at least **USD 7 bn by 2034[53].** In November 2024, Analysys Mason predicted even higher figures, up to USD 10 bn in 2029.

While the EU has good presence and strengths in the submarine/backbone networks market, it faces strong and increasing pressure from global competitors. Current market trends show a steady decline in European investment, leading to the exit of European actors and a loss of EU market share[54]. Meanwhile, the US continues to invest in **high-capacity backbone networks**, driven largely by hyperscalers, content providers, and cloud companies.

Between 2019 and 2023 the amount of international submarine cable capacity deployed by GAFAM (Google, Apple, Facebook, Amazon, Microsoft) quadrupled. Today, Google, Meta, and Amazon own 59 international submarine cables, up from just 20 in 2017, meaning that the bulk of **capacity is now held by non-EU controlled companies.**

In terms of cable manufacturing and deployment, the main US player, SubCom, has the greatest market share worldwide, followed by French-owned Alcatel Submarine Networks (ASN) and Japan's NEC. China's Huawei Marine Networks (HMN) is lagging behind but is gaining market share rapidly. Additionally, the US and Japan have recently announced massive investments in deployment capacities (including

[53] FSISAC, Critical Guidance report on Subsea Cable Risks for Financial Firms, 2024.

[54] Future Market Insights report, Submarine Communication Cables Market Size & Growth 2034

icebreaker vessels). The EU Risk Assessment published by the Commission in October 2025 provides a full analysis of the market and stakeholder ecosystem[55].

Given their criticality and of the rapidly evolving markets that determine network topography, capacity, but also resilience, security and control, the EU has paid increasing attention to backbone networks and in particular **submarine cables,** proposing a comprehensive policy approach, including regulatory and funding measures.

On the policy side, the EU Action Plan on Cable Security has outlined a series of coordinated actions to address risks and enhance the security and resilience of data and power submarine cable infrastructures, across the full resilience cycle: prevention, detection, response and recovery, and deterrence[56]. To support the implementation of the 2024 Cable Recommendation[57] and 2025 Action Plan, the Commission set up the Submarine Cable Infrastructures Expert Group and published in October 2025, its EU risk assessment (based on threats, vulnerabilities and dependencies), including mapping and stress test guidance on the security and resilience of EU submarine cable infrastructures[58].

Furthermore, on 5 February 2026 the Commission published the Cable Security Toolbox, which recommends a set of mitigation measures to address the identified risk scenarios, as well as a list of Cable Projects of European Interest (CPEIs), *i.e.,* areas to be prioritised for public funding[59].

On the funding side, to date the EU **invested over EUR 600 million** in more than **70 Digital Global Gateways** projects through the Connecting Europe Facility Digital programme (CEF Digital). While a number of satellite-terrestrial links and cross border terrestrial backbone projects have been funded, the vast majority of the funding was dedicated to submarine cable projects (59 projects for EUR 548 million). These projects are enabling significant improvements in the coverage of islands and remote territories, reduce vulnerabilities and risks, while increasing the overall resilience and redundancy of connectivity systems within the EU and linking the EU to the world, contributing to strategic objectives such as the connection of Europe to Asia through the Arctic, including Greenland's and other areas identified in the CPEI list.

In line with the EU Action Plan on Cable Security, the Commission amended the CEF Digital Work Programme, in February 2026, allocating EUR 347 million to fund strategic submarine cable projects[60]. These calls will support the CPEIs, including to enhance the EU's cable repair capacity, and equip submarine cables with smart capabilities.

---

[55] European Commission, Security of Cables: Commission publishes landmark report and funding for Cable Hubs, October 2025.

[56] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to Strengthen the Security and Resilience of Submarine Cables, JOIN(2025) 9 final, 2025.

[57] European Commission, Commission Recommendation (EU) 2024/779 of 26 February 2024 on Secure and Resilient Submarine Cable Infrastructures, 26 February 2024.

[58] European Commission, Security of Cables: Commission publishes landmark report and funding for Cable Hubs, October 2025.

[59] European Commission, Submarine Cable Security Toolbox and Cable Projects of European Interest, February 2026.

[60] European Commission, Commission increases submarine cable security with €347 million investment and new toolbox, 2025.

In 2026, two funding calls worth EUR 60 million will support cable repair modules, alongside a separate EUR 20 million call for SMART cable system equipment. These are sensors and monitoring components integrated into submarine telecommunications infrastructure to gather real-time ocean and seismic data. Additionally, two calls for new CPEI cables are planned for 2026 and 2027, with a total budget of EUR 267 million.

However, while CEF has already intervened in the CPEI areas, and will continue to do so in an increasingly focused manner, the remaining funding capacity of CEF Digital remains modest compared to the total investments needs. This gap is also reflected in the increasingly high oversubscription rates in CEF Global Gateway calls[61]. Cost estimates for deploying CPEI projects exceed EUR 10 billion[62]. Other studies suggest that at least a threefold increase of the current level of funding per annum for submarine cables (i.e. EUR 200 million) will be needed to maintain the current level of European ownership in the cable market and give greater scope and ambition to address market fragilities and critical capability gaps.

It is therefore important that support continues for the deployment, upgrade and maintenance of submarine cables to preserve competition and foster increased reliability and security standards. Deploying submarine cables and equipping them with advanced security monitoring and rapid-repair capabilities remains vital and requires continued public funding in the next MFF. In line with the Cable Security Toolbox, this intervention must focus on routes that are strategic for the EU (CPEI areas) and reduce reliance on non-EU suppliers.

In parallel, the **DNA introduces new provisions concerning the resilience of electronic communications networks and services.** These include cooperation and coordination of resilience and preparedness actions, data collection, early warning, networks' resilience mapping and networks' capabilities to ensure the redundancy through different types of networks' backups. The purpose is to **identify potential bottlenecks where resilience-enhancing measures are needed at Union level, including strategic investments to support redundancy, in particular, for trans-European digital networks**.

In this context, the newly proposed Office for Digital Networks (ODN) will be tasked, once the DNA proposal is adopted, with ensuring a coherent, cross-border approach for electronic communications networks and services, among others by preparing the **Union Preparedness Plan for Digital Infrastructures**, which will include a comprehensive assessment and an overview of network topology at Union level, identify route diversification, potential bottlenecks or points of failure and areas where resilience-related measures, such as strategic investments to support redundancy, are needed.

Such information, especially on integrated connectivity covering a wide range of terrestrial and non-terrestrial communications networks, can support **a wider analysis, complementing the one which led to the Cable Projects of European Interest,** and thereby ensuring **an updated, integrated prioritisation of**

[61] European Commission, Progress Report on the Implementation of the 2021–2027 Connecting Europe Facility for the Years 2021–2024, COM(2025) 516 final, 24 September 2025.

[62] European Commission, Submarine Cable Security Toolbox and Cable Projects of European Interest, February 2026.

critical investments in strategic backbone networks. Building on broader orientation set out in the Council conclusions on Connectivity of 6 June 2025, the Council also invited the Commission to assess the possibility of a coordinated initiative for planning and developing a reliable and resilient network of digital infrastructures and capacities, including backbone terrestrial, submarine and satellite networks, across the Union and with international partner countries.

Recommendation:

Member States should accelerate the deployment of secure and resilient connectivity infrastructure across the Union, by:

(i) cooperating within the Cables Expert Group to implement the Cable Security Toolbox, to advance the deployment of Cable Projects of European Interest, and assess future priorities;

(ii) building on the CPEI approach, analyse needs and links to other types of networks, taking into account projected AI data centre and cloud needs and pooling funding resources at national and EU level to deliver end-to-end resilient, secure and redundant connectivity infrastructure;

(iii) supporting the rollout of high-quality 5G stand-alone and 6G across the EU, including by assigning, defining sharing conditions or renewing spectrum rights under investment-conducive conditions, with particular attention to the 3.8-4.2 GHz band for local private networks;

(iv) should actively contribute to 6G development in Europe, in particular by promoting EU capacities in 6G and related technologies (semiconductors, quantum, AI, cloud), supporting R&I funding and pilots (together or in coordination with the European Commission and the SNS JU).

(v) supporting the coordinated deployment of low-latency and high-speed secure satellite connectivity in multiple orbital layers, as a resilient and secure complement to terrestrial connectivity;

(vi) continuing the expansion of fibre networks through coordinated funding and regulation, with particular attention to underserved and rural areas, and actively promoting the switch-off of copper networks where FTTH coverage has reached around 95% and comparable retail offers are available;

(vii) strengthening joint efforts to improve network coverage by supporting, via targeted funding and appropriate regulatory intervention, as appropriate, end users'' connections.

2.2.2. Digitalisation of SMEs and uptake of digital technologies by EU enterprises: AI, Cloud and data analytics

While building cutting-edge capacity and infrastructure is a necessary condition for digital competitiveness, **the diffusion and deployment of advanced technologies across businesses is key to ensure that technological leadership translates into competitiveness gains.**

The broad diffusion of technologies across firms, sectors and regions is therefore a second fundamental challenge facing the EU, and a key driver for productivity growth and economic transformation. The data on cloud, data analytics and AI up-take confirm that headline adoption figures are moving in the right direction, but progress is too slow relative to 2030 targets, and SMEs consistently lag behind large enterprises.

The percentage of SMEs with at least a basic level of digital intensity, according to version III of the Digital Intensity Index, rose by 13.5 percentage points in two years, from 57.90% in 2023 to 71.38% in 2025. This reflects a year-on-year increase of 11.0%.

According to the forecast along the baseline trajectory, the target is expected to be achieved and surpassed by 2030, with an estimated 92.08% of SMEs having at least a basic value of the digital intensity index by then (Figure 5). The revised baseline trajectory is fully in line with the ideal trajectory. In 2025, the observed and ideal values overlap almost perfectly.

In their National Roadmaps, **165 measures corresponding to a total of EUR 48.4 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.

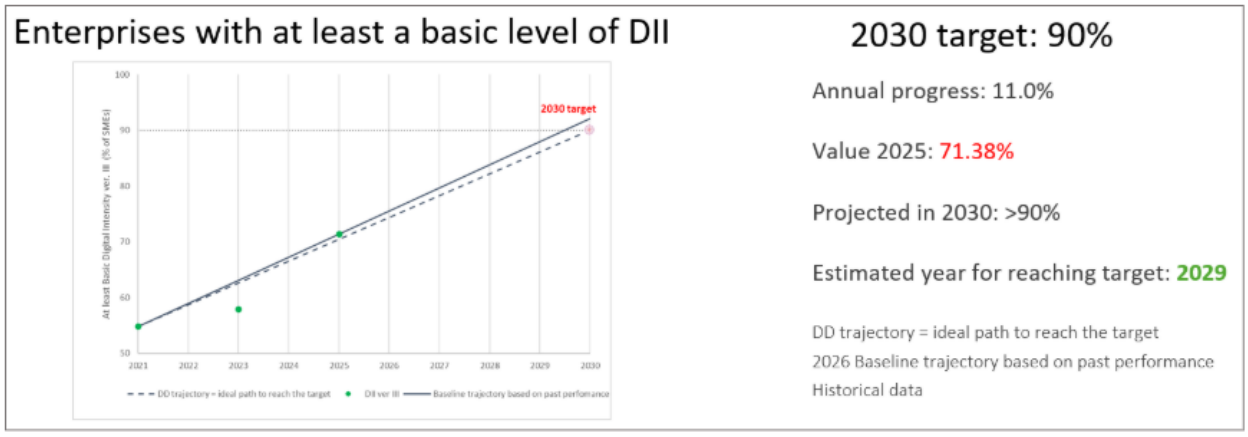


Figure 5: Digital Intensity Index ver. III. Digital Decade (DD) trajectory and revised baseline trajectory towards 2030.

The percentage of enterprises using at least one of the three technologies (Cloud, Data Analytics or AI) rose by 8.5 percentage points, from 54.7% in 2023 to 63.20% in 2025. This represents a substantial year-on-year increase of 7.5%.

According to the forecast along the revised baseline trajectory, 95% of the target is expected to be achieved by 2030, with 71.5% of enterprises expected to use at least one of the three technologies by then (Figure 6). In 2025, the value of this KPI aligns perfectly with the ideal trajectory, reaching a value of 63.2%. The target of 75% of enterprises using at least one of the three technologies is expected to be reached in 2033 if no further actions are taken.

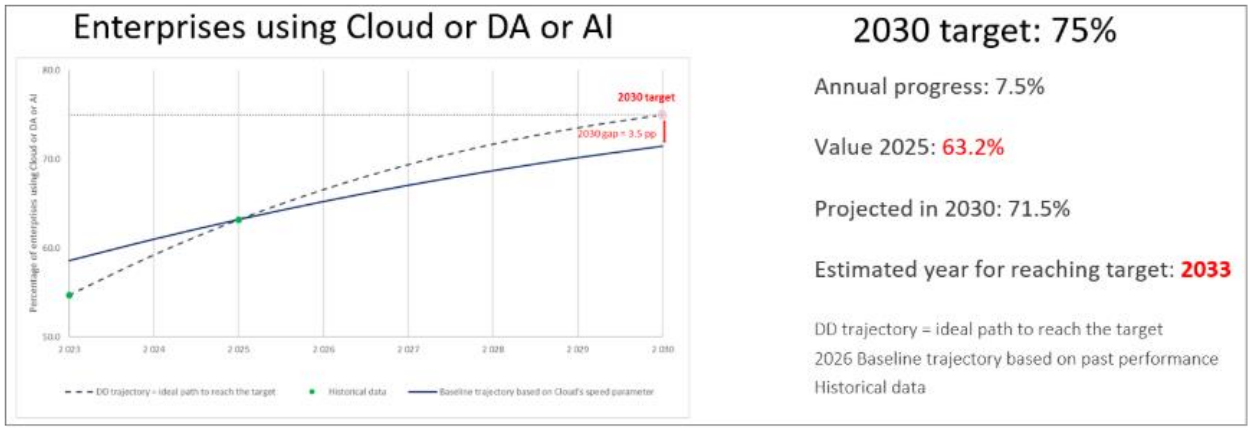


Figure 6: Percentage of enterprises using AI or cloud computing or data analytics in the EU. Historical data, Digital Decade (DD) trajectory and baseline trajectory towards 2030 (same speed of diffusion parameter as in cloud baseline trajectory).

Artificial Intelligence

According to Eurostat data, the percentage of enterprises using AI technologies rose by 6.5 percentage points in one year, from 13.5% in 2024 to almost 20.0% in 2025. This represents a substantial year-on-year increase of 48%, however lower than the 67% year-on-year increase of 2024.

In EU companies, the most widely used AI technologies are those for analysing written language (11.8%), which also saw the strongest increase since 2024. They are followed by AI for generating images, videos or audio (9.5%), producing written or spoken language (8.8%), and converting speech into machine-readable format (7.2%). According to the forecast along the baseline trajectory, 72% of the target is expected to be achieved by 2030, with 54.28% of enterprises expected to adopt AI by then (Figure 7). In 2025, this KPI reached a level slightly above half of the ideal value defined by the ideal trajectory (at almost 20.0% instead of 39.1%). The target of 75% of enterprises using AI is expected to be reached not earlier than 2035 if no further actions are taken.

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 3.8% of the total budget across roadmaps and covering 199 measures in total. Among these, roughly 34 measures specifically target AI,

accounting for EUR 1.4 billion. 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, AI-specific measures place a stronger emphasis on building AI capabilities. This focus is also reflected in Member States' roadmap adjustments.

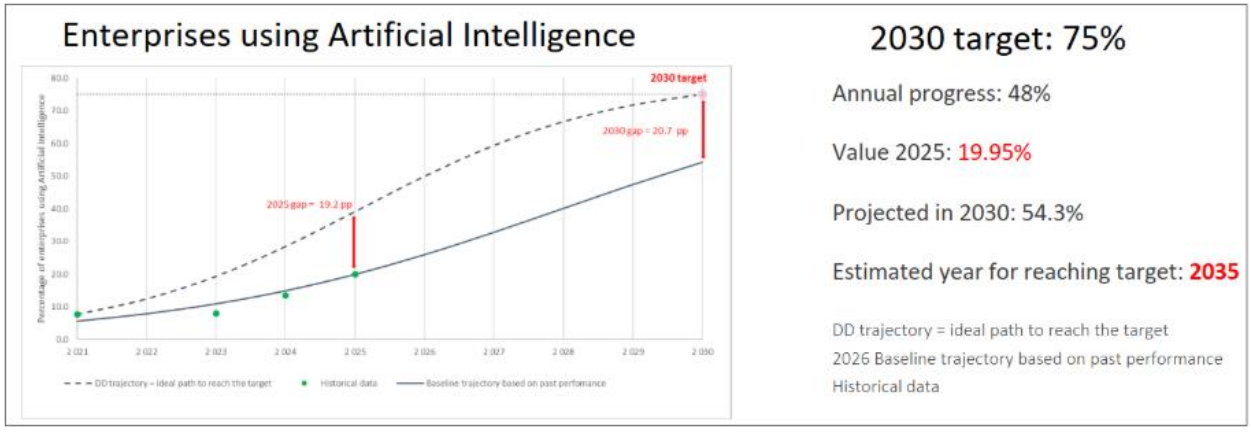


Figure 7: Percentage of enterprises using AI in the EU. Historical data, Digital Decade (DD) trajectory and revised baseline trajectory towards 2030.

These figures indicate that, despite strong recent progress, including on policy making at EU and national level, the EU remains below the Digital Decade target. Reaching 75% of enterprises by 2030 will require targeted support, especially for SMEs and for sectors and regions that lag behind. They also show that large firms still adopt AI much faster than SMEs, even if smaller firms are accelerating.

For European SMEs, the evidence suggests that the main obstacle is no longer basic awareness of AI but the difficulty of turning interest and pilots into broad business deployment. Eurostat's latest statistics support this analysis. Among EU enterprises that had considered using AI but did not adopt it, the main reasons reported were lack of relevant expertise (70,89%), lack of clarity about legal consequences (52,52%) and concerns regarding violation of data protection and privacy (48,83%). For many firms the issue is no longer whether AI matters, but whether they can implement it safely, lawfully and effectively.

Concretely, for SMEs, the most recurrent bottlenecks are fragmented and poor-quality data, weak interoperability systems, lack of in-house skills, uncertain returns on investments and difficulties in integrating AI in core business processes. These barriers are compounded by organisational and compliance difficulties, with many SMEs not having the internal capacity to identify viable use cases, adapt workflows, assess risks, or manage legal uncertainty around data use and AI deployment.

The main challenge is therefore one of scale and broad-based diffusion across industrial sectors with particular focus on the strategically important ones.

For instance, the OECD Study[63] - indicates that in manufacturing, AI uptake is still "*modest and highly fragmented*": the share of manufacturing enterprises using at least one AI technology rose from 7% in 2021 to 11% in 2024, but the technology is still not well integrated into core production processes. The most common uses are still language-based and administrative tasks, while uptake remains lower for functions more directly tied to production, such as image recognition, robotic process automation and machine-learning-based optimisation.

In public transport and logistics, the report finds that many deployments remain at pilot or early implementation stage and that SMEs often struggle to keep pace because of limited access to expertise, infrastructure and funding.

Across sectors, the OECD repeatedly identifies fragmented datasets, poor interoperability, integration into legacy systems, compliance complexity and weak internal skills as persistent constraints on scaling.

For SMEs, **de-risking adoption** has become essential: they need trusted intermediaries, simpler access to expertise, and support that combines technology, compliance and business transformation rather than addressing these issues separately. This is consistent with the direction already taken by the **Apply AI Strategy**, which includes the role of the **European Digital Innovation Hubs (EDIHs)** as **Experience Centres for AI** and as key partners helping SMEs to "*test before invest*", identify funding for their AI projects or network within the AI ecosystem of AI factories, Testing and Experimentation Facilities (TEFs) and future national sandboxes.

At the national level, by the turn of 2026, the vast majority of Member States have already adopted and/or revised their own national AI strategies. However, the national implementation remains uneven in terms of dedicated budget allocated, measurable KPIs or regular evaluation.

For instance, funding AI at national level is highly uneven and often difficult to isolate because many AI measures are combined with wider digitalisation plans. This creates a divide between countries with operational governance, measurable follow-up and financing mechanisms for AI and those where AI remains embedded in broader agendas without a strong delivery architecture. Moreover, some member states do not use well-defined KPIs for AI strategies, using instead broad digital transformation frameworks.

At European level, stronger coordination is needed to connect strategy, infrastructure and deployment. The **AI Continent Action Plan** provides the upper-level framework for the infrastructure and enabling layer, notably through AI factories, high-quality data access and compute capacity. The **Apply AI Strategy** is particularly important for the uptake objective, as it is explicitly the EU's overarching sectoral AI strategy and is designed to boost adoption and innovation across Europe, especially among SMEs. In this architecture, **EDIHs** are meant to function increasingly as **AI Experience Centres** linked to AI Factories,

[63] OECD Study - Progress in Implementing the European Union Coordinated Plan on Artificial Intelligence. Uptake in high-impact sectors / volume 2

Testing and Experimentation Facilities (TEFs) and regulatory sandboxes, while the **AI Skills Academy** supports the workforce dimension.

For AI uptake in EU companies, this EU-level coordination is critical: Member States on their own cannot efficiently provide the full combination of compute, high-quality data, regulatory support, testing infrastructure, skills and cross-border market scale needed for rapid AI uptake. Related to the regulatory framework, national market surveillance authorities, which each Member State is required to designate under the AI Act, are responsible for enforcing compliance with the rules applicable to AI systems, including by proposing joint investigations with the European Commission. To the best of our knowledge, 10 Member States (Denmark, Finland, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, Slovenia and Slovakia) have designated their national market surveillance authorities[64]. The timely establishment of these authorities, together with sufficient technical, financial and human resources, will be critical to ensuring robust oversight and effective enforcement of the AI regulatory framework.

The urgency is clear when current performance is compared with EU ambitions. Reaching the AI targets will depend on aligning reforms and investments across all levels of responsibility (European, national, regional and local) around a key objective: **making AI adoption easier, safer and more affordable for EU companies, especially SMEs**.

Recommendation:

Member States should support the development, deployment and wide uptake of AI through a coordinated industrial, public-sector and governance strategy. In particular, they should:

(i) adopt and implement national AI strategies grounded in the "AI-first principle", where appropriate, as proposed in the Apply AI strategy, with clear priorities for industrial competitiveness, public-service transformation and innovation diffusion;

(ii) strengthen investment in the development and deployment of AI models, systems and infrastructure relevant to strategic sectors such as automotive, manufacturing, healthcare, mobility and energy, while also addressing physical AI systems that integrate perception, reasoning and action in real-world environments, including robotics;

(iii) support the real-life deployment of connected and autonomous vehicles, unmanned aerial systems, drones and cooperative drone swarms, in collaboration with regional and local authorities, and prioritise European technologies, while promoting EU initiatives such as Autonomous Drive Ambition Cities and the Drones Action Plan

(iv) support European participation in and access to frontier AI development - including large-scale advanced models and next-generation multimodal systems - by investing in computing

[64] Cut-off date 27 April 2026.

infrastructure, and fostering public-private partnerships with AI developers, with national contributions feeding into a coordinated EU-level effort;

(v) identify, pilot and scale high-impact AI use cases across the public sector, including open-source applications made in Europe;

(vi) continue supporting the network of European Digital Innovation Hubs ("Experience Centres for AI"), which play a key role in accelerating the uptake of AI and other digital technologies, particularly among SMEs and public administrations;

(vii) ensure that national and regional AI initiatives are integrated into the broader EU AI ecosystem - including Experience Centres for AI, AI factories, regulatory sandboxes, Testing and Experimentation Facilities (TEFs), and EU Digital Skills Academies - to avoid duplication, pool resources and ensure that European firms can access world-class infrastructure, expertise and compute capacity;

(viii) put in place comprehensive measures to strengthen AI literacy and advanced digital skills across society, including for workers, citizens and public administrations; and

(ix) operationalise the AI Act by establishing the necessary national governance and support structures - including market surveillance authorities, single points of contact, regulatory sandboxes, and accessible compliance guidance for SMEs - ensuring that conformity assessment, post-market monitoring and incident reporting obligations are matched by adequate national technical capacity.

Cloud computing services

The percentage of enterprises using sophisticated or intermediate cloud computing services rose by 7.7 percentage points, from 38.97% in 2023 to 46.69% in 2025. This represents a **year-on-year increase rate of 9.5%**. According to the forecast along the updated baseline trajectory, **approximately 81% of the target is expected to be achieved by 2030,** with 60.6% of enterprises estimated to adopt sophisticated or intermediate cloud services by then (Figure 8). The target is expected to be reached not earlier than **2040,** if no further actions are taken.

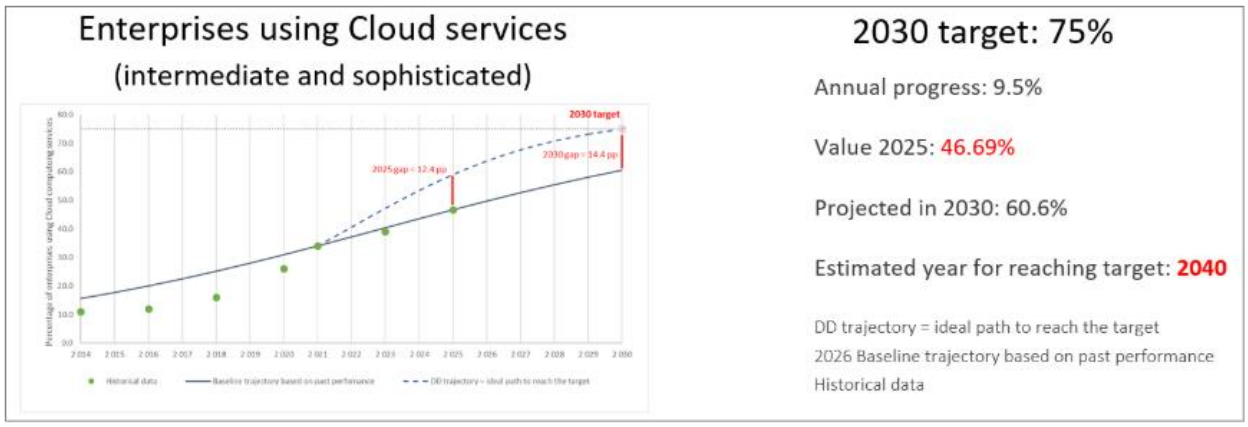


Figure 8: Percentage of enterprises using intermediate and sophisticated cloud computing services in the EU. Historical data, Digital Decade (DD) trajectory and revised baseline trajectory towards 2030.

Cloud computing remains critical for business digitalisation and is becoming an increasingly relevant enabler for AI deployment and uptake. Around 53% of enterprises used paid cloud computing services in 2025, an increase of around 8 percentage points with respect to 2023[65]. However, the most advanced end of this adoption is less widespread, with approximately 41% of enterprises buying at least one sophisticated cloud service. This demonstrates that adoption is growing but most firms are still using basic services. Cloud uptake is advancing but too slowly relative to the ambition of the 2030 target, which makes this recent acceleration not sufficient on its own.

One of the factors holding back progress is the persistent SME gap. In 2025, 46% of SMEs used cloud services, compared with 60% for enterprise 50-249 employees and 78% of large enterprises. The comparison across countries is equally significant, with Finland's SMEs reaching 72% of average cloud uptake while Romania, Greece and Bulgaria remaining below 25%.

To close this gap, policy support needs to target late adopters, especially SMEs, through practical support and advisory services. Stronger enforcement and implementation of the switching rules under the Data Act, entered into force in September 2025, could also help firms switch providers more easily and adopt cloud with lower lock-in risks. Progress towards the target will depend both on demand-side incentives, especially for these lagging groups and on whether the EU can build a sufficient, secure and sustainable computing infrastructure to accompany this transition. Without this combination, cloud uptake may continue to rise, but as shown above, too slowly to achieve the 75% target by 2030.

Finally, cloud can be considered an essential enabler for the uptake of data analytics and AI services, detailed below. For this potential to materialise, more firms will have to move from basic cloud consumption to more advanced data and AI-related uses.

[65] Eurostat, Cloud Computing Statistics – Enterprises, 2026.

Data Analytics

The share of enterprises using analytics rose from 33.25% in 2023 to 39.85% in 2025, an increase of 6.6 percentage points. Despite this progress, the EU remains off track to meet the Digital Decade target by 2030: under the revised baseline trajectory, only 51.9% of enterprises are expected to use data analytics by 2030, corresponding to around **69% of the target, and the** target would be reached only by **2047** in the absence of additional action.

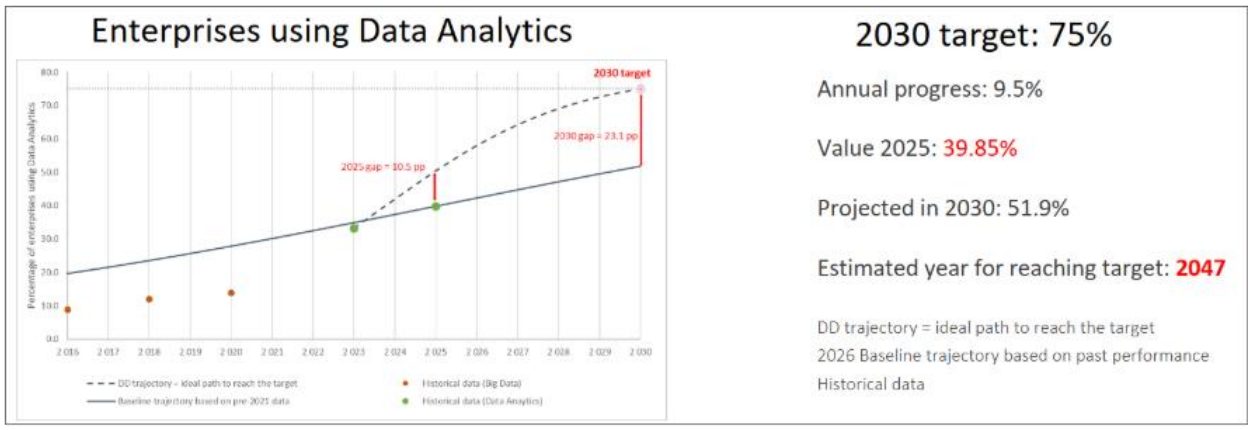


Figure 9: Share of enterprises using Data Analytics in the EU. Historical data, Digital Decade (DD) trajectory and baseline trajectory towards 2030.

The EU has laid important foundations for the data economy through the European Strategy for Data and related key legislative instruments such as the Data Governance Act, the Data Act, and the Open Data Directive. However, significant barriers continue to limit the wider uptake of data analytics by enterprises, especially SMEs.

A first major challenge is **data scarcity and limited access to high-quality datasets** for data analytics and AI development. Valuable datasets remain siloed within organisations, fragmented across sectors, or difficult to access across Member States' borders. This particularly affects start-ups and SMEs, which often lack access to sufficiently large, high-quality datasets and the computing resources needed to use them effectively. As global competition intensifies, broader and more reliable access to quality data becomes increasingly important for innovation and competitiveness.

A second challenge is **regulatory complexity and fragmentation**. The EU has developed a broad framework governing data access, sharing and protection, but interaction between horizontal and sectoral rules, combined with uneven implementation across Member States, can generate legal uncertainty and increase compliance costs. This is particularly burdensome for SMEs and emerging data intermediaries and can slow the scaling-up of data-driven business models and European data ecosystems.

A third key challenge is the **strategic and geopolitical dimension of data**. Data has become a key economic and security asset. Jurisdictional issues remain a critical concern. Data held by companies subject to non-EU jurisdictions may be accessed by foreign authorities, including under extraterritorial legal frameworks

such as the US Cloud Act. This raises questions about effective control, legal certainty and the enforceability of EU rules, particularly for sensitive or strategic datasets. European firms must be able to benefit from secure cross-border data flows and access to global data resources, while the EU must also protect sensitive and strategic datasets and ensure that data governance remains consistent with European values.

Addressing these barriers will require coordinated reforms and investment. Priority actions include **scaling up access to high-quality data for AI and innovation at large**, notably through the further deployment of **common European data spaces and** strengthening interoperability through open and modular solutions. Linking data spaces with **data labs and AI factories** could help transform Europe's data assets into resources for trustworthy AI and advanced analytics.

Further efforts are needed to **simplify and modernise the EU data regulatory framework**, making it clearer, more innovation-friendly, and less burdensome for businesses, especially SMEs. In this context, the proposed **Digital Omnibus** aims to streamline existing data legislation by reducing overlaps, updating certain rules (including on privacy and data use), and clarifying the implementation of key instruments such as the Data Act, while preserving their core objectives.

Strengthening EU data sovereignty and fair international data flows also remains essential. This requires enabling cross-border access to data, improving access to larger and more diverse datasets for businesses, and addressing remaining barriers to data sharing. Such measures are critical to support the development of advanced data analytics and AI applications and to enhance the global competitiveness of European companies.

Recommendation:

Member States should support the uptake of cloud, AI and data analytics by enterprises, in particular SMEs and start-ups and government services in line with the proposed Cloud and AI Development Act, the Apply AI Strategy and the EU data acquis, by:

(i) ensuring a consistent and business-friendly implementation of EU data rules and improving access to high-quality data, computing resources, data labs and innovation support services;

(ii) accelerating the deployment of common European data spaces and strengthening interoperability through open and modular solutions, in particular through the relevant European Digital Infrastructure Consortia (such as ALT-EDIC, and the upcoming Mobility and Logistics EDIC and Agri-food EDIC);

(iii) reinforcing data sovereignty and secure cross-border data flows, in support of the development of trustworthy AI in the EU and the global competitiveness of European firms;

(iv) facilitating the adoption of secure, open and efficient cloud computing services by SMEs, companies in sectors of high criticality in line with NIS2, and government services through targeted support, resources and incentives that overcome barriers to adoption, including skills, resources and awareness.

2.2.3. Open Source

Open source is a strategic enabler of the digital transformation of the European Union and the Digital Decade goals as it underpins most modern digital systems and directly affects Europe's competitiveness, resilience and technological sovereignty. **Open source makes up 70 to 90% of all code in the digital economy**[66]. A 2024 Harvard Business School study[67] estimated the demand-side value of open-source software at USD 8.8 trillion and found that firms would need to spend 3.5 times more on software if open source did not exist. The EU starts from a position of strength, with more than 3 million open-source contributors, more than 500 for-profit open-source companies and substantial EU support to open-source actions across cloud, AI, cybersecurity, internet technologies and chips, estimated at around EUR 800 million in the current MFF. Yet these strengths are still not converted into sufficient market scale, stewardship capacity or control over critical parts of the digital stack.

The main hurdles are structural. First, the EU still struggles to move from research and community development to adoption at scale. Many promising projects lack financing for integration into real-world environments, user experience improvements, security hardening, performance testing, legal compliance and commercial deployment. Second, maintenance remains a major market challenge. Critical open-source components are often widely used but maintained with fragile resources, creating both security and continuity risks. Third, access to scale-up capital remains weak, particularly for European SMEs and mid-caps building open-source business models. Fourth, public procurement frameworks still tend to favour incumbent proprietary suppliers by focusing on short-term pricing, product bundles and vendor-specific features rather than lifecycle cost, interoperability, exit costs and strategic control. Fifth, the EU still lacks sufficiently strong stewardship, governance and trust organisations that can carry out assessments, security attestations to make open software easier to buy and deploy in regulated or mission-critical environments. These challenges are amplified by fragmentation across Member States and by continued dependence on non-EU digital infrastructures and services, including software repositories, code hosting platforms, cloud execution environments and trust services that remain outside EU jurisdiction.

Investments and reforms are therefore needed to address this situation. Public procurement should better recognise open standards, interoperability, reusability and total cost of ownership, including switching and lock-in costs so that open software can compete on equal terms in tenders. Public administrations should be supported with common guidance, model clauses and skills to be able to migrate to open-source solutions with confidence. The EU should also strengthen trust and adoption mechanisms by developing shared assessments and security assurances, promoting common catalogues,

[66] Synopsys, Open Source Security and Risk Analysis (OSSRA) Report, 2024; Hoffmann, M., Nagle, F., and Zhou, Y.

[67] "The Value of Open-Source Software," Harvard Business School Working Paper No. 24-038, 2024.

rolling out interoperability frameworks and reusing open digital building blocks across borders. The open-source licensing requirement for the EU Digital Identity Wallet and the launch of the Digital Commons EDIC show that the EU already has practical anchors on which to build a more coherent adoption strategy.

Investment needs should be organised across the full lifecycle of open software. This includes R&I funding for strategic open technologies, but also dedicated uptake and support, multiannual maintenance funding for critical components, and financing for European stewardship structures. In this respect, the proposed European Competitiveness Fund is highly relevant. With a budget of EUR 234 billion overall and instruments designed to combine guarantees, financial instruments, blending, support to start-ups and scale-ups, and advisory services, it could help address the current gap between technical excellence and market deployment. For open software, priorities should include supporting deployment-ready sovereign solutions in strategic domains; de-risking adoption by public administrations and SMEs; financing maintenance and security of critical dependencies; and mobilising equity, quasi-equity, guarantees and advisory support for European open-source firms and integrators. This would make open software easier, safer and more attractive to deploy at scale across the Single Market.

EU Open-Source Strategy will review the current state of play and put forward a set of actions to be rolled out in the coming years by the public sector at European and Member State level, as well as the private sector and the open-source communities themselves.

Recommendation:

Member States should mainstream open source as a strategic sovereignty instrument, by:

(i) defining national open-source strategies and a monitoring mechanism to track implementation, as an instrument for joint development of pre-competitive digital building blocks among European industrial actors;

(ii) engaging in cross-border collaboration through the Digital Commons EDIC (DC-EDIC), in particular by developing joint mechanisms to enhance the reusability, interoperability and cost-effectiveness of open-source solutions;

(iii) raising awareness across national and local public administrations and developing technical and operational skills, in particular through Open-Source Programme Officers (OSPOs);

(iv) Striving for an 'open source first' principle in public procurement, and where relevant making publicly funded software available for reuse;

(v) mainstreaming open source in national R&I programmes and in school and university curricula;

(vi) assessing barriers to open-source uptake, including cultural resistance, skills gaps and resource constraints, and putting in place targeted measures to address them.

2.2.4. Unicorns

The number of unicorns rose by 30 units (net increase), from 294 in 2024 to 324 in 2025, corresponding to 64.8% of the EU target. This represents a significant year-on-year increase of 10.2%. According to the forecast along the revised linear baseline trajectory, 88.0% of the target is expected to be achieved by 2030, with 440 unicorns expected to be active in the EU by then (Figure 10). The target of 500 unicorns, set in the 2023 Communication on EU-level trajectories, is expected to be reached in 2033 if no further actions are taken.

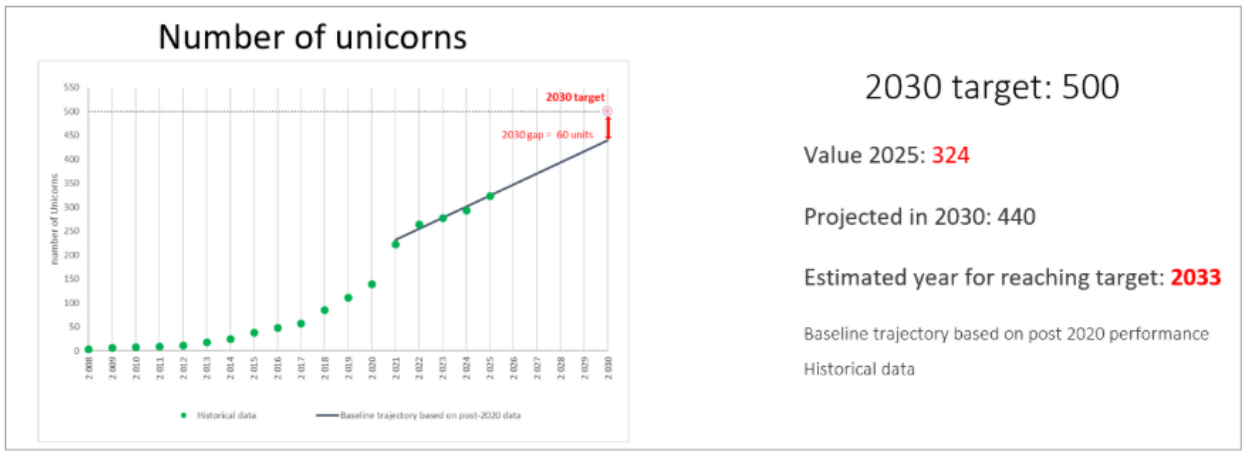


Figure 10: Number of unicorns in the EU. Historical data and revised baseline trajectory.

Newly released data confirms the post-2020 linear trend but also point to an acceleration in the creation of new unicorns. In 2025 was almost twice as much than those created in 2024, the EU recorded 30 new net unicorns in 2025 compared to 16 the previous year. The yearly rate of progression has increased from 5.8% in 2024 to 10.2% in 2025 (Figure 11).

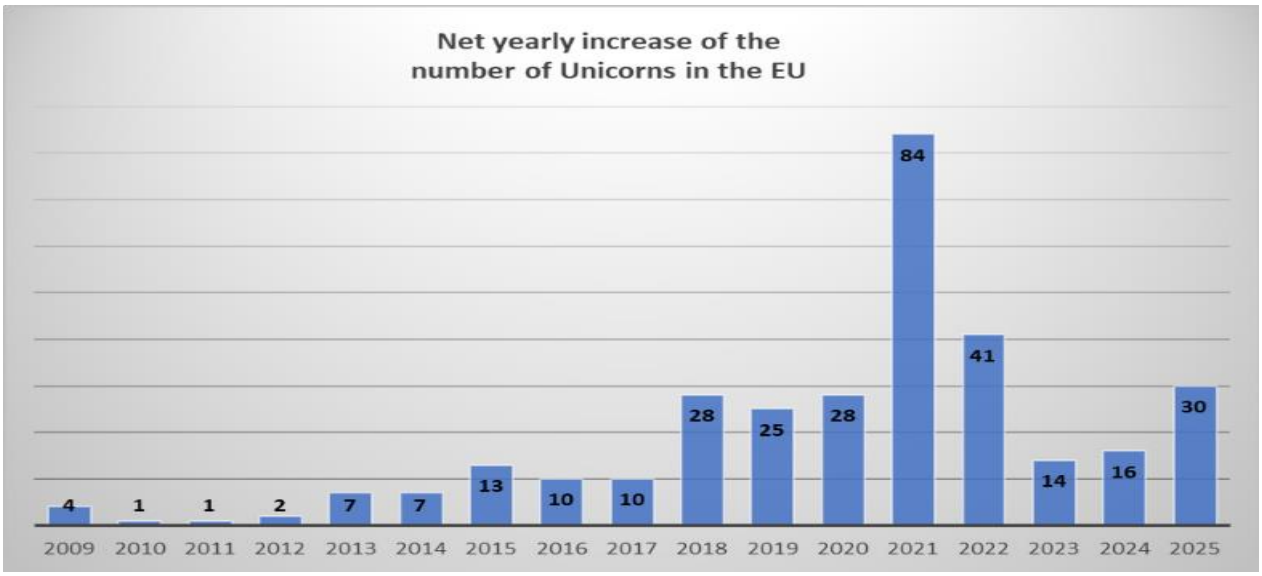


Figure 11: Number of unicorns in the EU by year: annual net increase (births-deaths) and relative annual progress since 2009.

Comparing the performance of the EU's startup ecosystem with that of its main global peers provides useful context for assessing its relative strengths and areas where further progress may be possible. Analysing the time series of unicorn creation since 2008 helps to place recent performance in a longer-term perspective and to compare the evolution of the EU's startup ecosystem with that of its main competitors - Canada, China, Israel, Japan, South Korea, United Kingdom and United States (Figure 12).

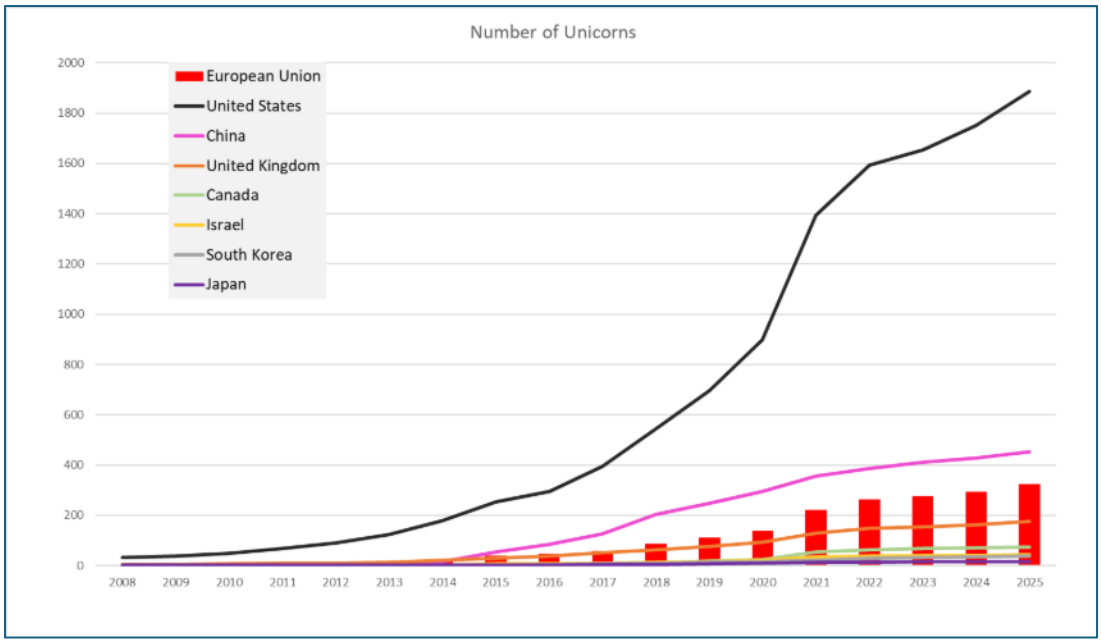
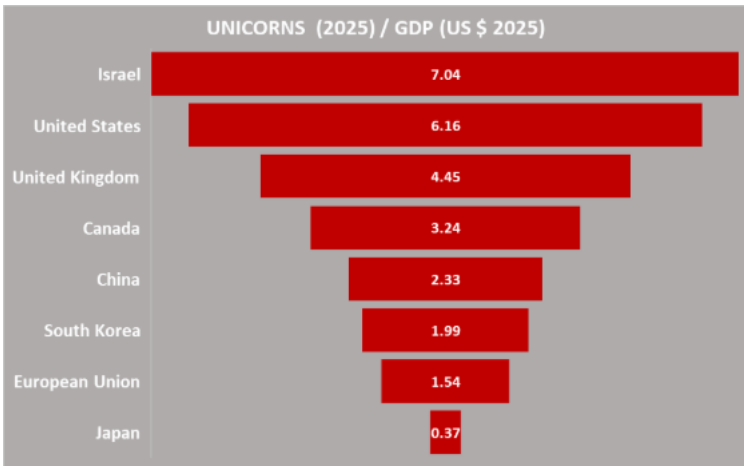


Figure 12: Number of Unicorns in the EU and its main competitors from 2008 to 2025.

The European Union expanded its unicorn base from 3 in 2008 to 324 in 2025, with growth accelerating after 2015 and again after 2020. Despite this progress, the EU continues to lag well behind the United States, which reached 1 886 unicorns by 2025 - almost six times the EU total - highlighting persistent gaps in market scale and late-stage financing. China number of unicorns was 40% higher than that of the EU in 2025 (452), while the United Kingdom alone accounts for more than half of the EU's unicorn total. Meanwhile, competitors such as Israel and Canada have scaled rapidly within large or well-integrated domestic markets.

Normalising the unicorn ecosystem by economic size confirms the EU's underperformance (Figure 13). Measured as the number of unicorns per USD 100 billion of GDP (2025 values)[21], the European Union records 1.54, well below Israel the top performer (7.04), the United States (6.16), the United Kingdom (4.45), Canada (3.24), China (2.33), and South Korea (1.99), while remaining above Japan (0.37). The gap with leading ecosystems such as the U.S. and Israel is sizeable, while the distance to countries such as the UK and Canada, though smaller, also remains noticeable. With an economy of around two-thirds the size of the U.S., the EU generates fewer than one-fourth as many unicorns per unit of GDP. It is also worth noting that the strong performance of the U.S. is highly concentrated geographically. California plays a disproportionate role in driving the U.S. unicorn ecosystem. Despite accounting for around 13% of U.S. GDP (40.5k billion in 2024, most recent available year[22]), California recorded 892 unicorns in 2025, representing almost half of all U.S. unicorns (1 886). This concentration highlights the importance of dense venture capital markets, leading technology hubs, and strong innovation networks, in shaping ecosystem performance.



GDP in Current prices, US dollar Year = 2025, Source: IMF	
Location	Billions
United States	30616
EU	21097
China	19399
Japan	4280
United Kingdom	3959
Canada	2284
Korea, Rep.	1859
Israel	611

Figure 13: Number of unicorns (2025) per economic size (GDP in US $ 100 billions).

Overall, the international benchmarking analysis points to a significant margin for improvement in the EU's ability to convert economic capacity into large-scale, high-growth firms if it is to narrow the performance gap with its global peers.

Tracking the outflow of EU-founded unicorns' relocation to third countries provides an important indication of the EU's capacity to retain high-growth innovative firms and to scale them within its own market[22]. The data show a gradual improvement in the EU's capacity to retain innovative scale-ups with respect to the U.K. and the U.S. over the past decade (Figure 14). Between 2016 and 2019, around one in five EU-founded unicorns relocated to the US or the UK, with percentages fluctuating between 21% and 22%. This indicates a relatively stable but significant outflow during that period. From 2020 onwards, the percentage of relocating companies declined more clearly and reached 16% in 2025. Other potential destination countries were also examined (Canada, China, Israel, Japan, South Korea), but no cases of relocation of EU-founded unicorns were identified outside the U.K. and the U.S. over the period considered.

The trend suggests a moderate but consistent strengthening of the EU's ability to retain its innovative scale-ups. While relocation remains a structural challenge, with roughly one in six unicorns still moving abroad, the outflow has decreased by around five to six percentage points compared to the 2016-2018 peak.

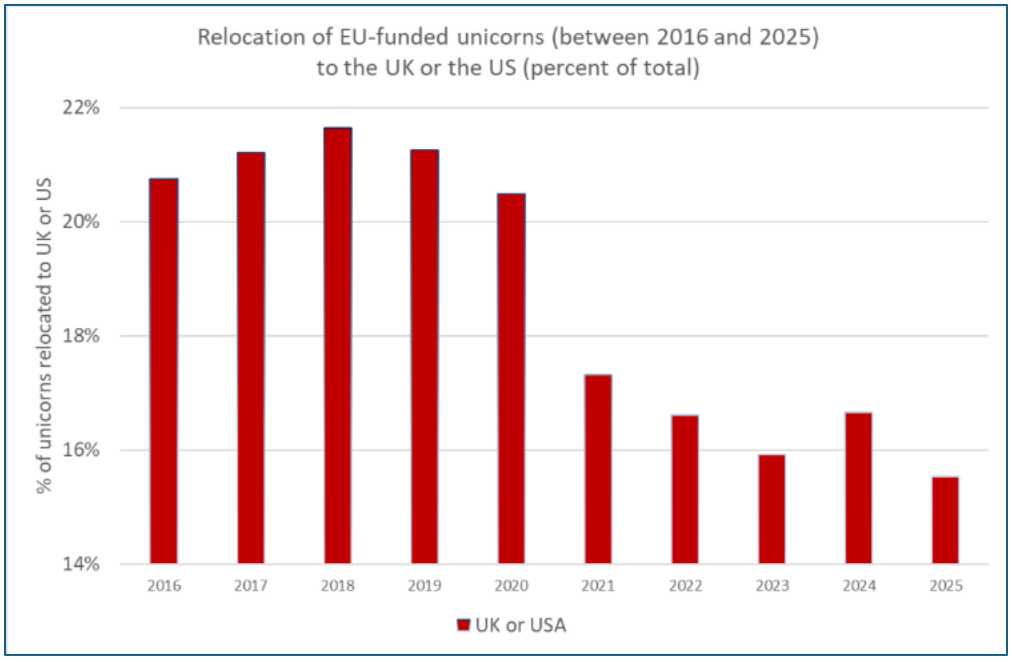


Figure 14: Percentage of unicorns founded in the EU in the past decade that later relocated to either the United Kingdom or the United States.

Challenges facing EU startups on the path to unicorn status

In the EU, the path from promising startup to unicorn presents obstacles that are often more pronounced than in other competing regions. Three non-exhaustive challenges stand out in particular: the scale-up funding gap, weak spinoff creation and tech transfer policies, as well as the difficulty startups face in accessing public procurement markets.

The most glaring obstacle is the lack of **late-stage capital** for startups seeking to raise EUR 100 million or more. While early-stage funding has improved, EU startups frequently hit a wall when they need large-scale investment to expand globally. Fund sizes in Europe are typically smaller than in the US, meaning that fewer EU firms can access the EUR 100M+ cheques needed for rapid scaling. This was to be seen in the period 2024-2025 when 54% of lead investors in late-stage VC investments in European AI Startups were from American investors. A result of this is that many EU startups either up either accept lower valuations or seek funding from non-European investors, too often resulting in relocation to the US. Compounding this issue is the fragmentation of Europe's capital markets that the EU's Saving and Investment Union Strategy seeks to address.

Another hurdle is Europe's volume of **spinoff creation and related tech transfer policies**, which can prevent groundbreaking research from reaching the market. The EU remains a global leader in R&D, with world-class universities and corporate labs, but it still lags the US in commercialising innovation. Many European universities have historically retained excessive ownership of intellectual property (IP) developed by researchers, discouraging academics from launching spinoffs, although recent years have seen encouraging progress in this area. When spinoffs do emerge, they often lack the funding, mentorship, or business expertise needed to scale.

Progress on tech transfer is systematically measured by the European Startup Network Alliance (ESNA) through its "Existence of Policies for Smooth Tech Transfer" indicator.

While ESNA's indicator shows Member States progressing in the aggregate, towards a "full" policy framework for spinoffs and tech transfer, there remain several opportunities to improve the conditions for spin-off creation and subsequent market growth. For example, Member States could further enhance conditions by:

- Mobilising government co-funding (grants, loan guarantees, or equity investments) for early-stage spin-offs to reduce risk for private investors.
- Encouraging undertakings of all sizes to invest in spin-offs through tax incentives, government grants, or direct partnerships
- Launching national or regional initiatives to encourage entrepreneurs (for example experienced startup founders) to work more closely with university researchers and contribute their expertise (including but not limited to mentoring of researchers open to entrepreneurial paths).

Another barrier is the difficulties EU startups face in accessing **public procurement markets**, which represent a EUR 2 trillion annual opportunity. Despite their innovative potential, SMEs and startups win less than 10% of public contracts, often because procurement rules and tender procedures are designed in ways that favour large incumbents. In practice, these processes tend to reward companies with long track records rather than younger and more agile firms.

Recommendation:
Member States should close the European scale-up gap, by:

(i) actively addressing the shortage of European capital for large investment rounds (above EUR 100 million), through public funding allocated to existing or new investment vehicles, including pan-regional funds, with EIB and EIF support, or by joining existing initiatives such as the European Tech Champions Initiative (ETCI 2.0);

(ii) initiating public-private partnerships that offer partial guarantees or shared-risk models to facilitate pension fund investment in start-ups and scale-ups;

(iii) accelerating spinoff creation and tech transfer, by mobilising government co-funding (grants, loan guarantees, equity) for early-stage spin-offs, by encouraging national leading companies and mid-caps to invest in the spin-off ecosystem (including via tax incentives), and by mobilising experienced entrepreneurs to mentor researchers open to entrepreneurial paths.

2.3. Ensuring security for competitive growth

The global cybersecurity landscape is being reshaped by growing geopolitical competition and concentrated digital supply chains, which create systemic vulnerabilities across global markets. Cybersecurity is moving toward AI-enabled attack and defence operations, with threat actors increasingly using automation, generative AI, and large-scale exploitation of cloud - edge infrastructures. Meanwhile, advances in quantum computing require an urgent global transition toward Post-Quantum Cryptography.

.

Similarly, the EU is facing a cybersecurity landscape shaped by the weaponisation of AI, ransomware, growing dependence on untrusted suppliers and a chronic shortage of security expertise. Sophisticated adversaries, including both state and non-state actors, are exploiting vulnerabilities in cross-border ICT infrastructures, automated decision systems and emerging technologies. In addition, there is a clear and urgent need to ramp up efforts on Post Quantum Cryptography transition.

Despite significant progress, Europe remains structurally dependent on non-EU cybersecurity suppliers, and European companies are underrepresented in global cybersecurity leadership. The European market continues to rely predominantly on non-EU industry actors.

According to the Digital Decade Eurobarometer 2026, 91% of Europeans think the EU should cooperate with Member States to reinforce cybersecurity and protection from online threats. In addition, 86% of respondents think the EU should prioritise investments in digital infrastructure and services that are developed and controlled in Europe, and 58% of them would be willing to switch to an EU-based digital service provider even if it means slightly higher costs, pointing to the greater security and reliability as the main motivation for doing so.

In their National Roadmaps, Member States reported 39 measures contributing to increased cybersecurity. Almost half of these measures are dedicated exclusively to cybersecurity, with a total budget of EUR 0.79 billion. The other measures have a broader scope, aiming to support several targets across all areas, with a total budget of EUR 6.8 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.

As geopolitical and economic tensions continue to intensify, cyber threats against the EU have further evolved, with espionage, pre-positioning, and disruptive operations increasingly integrated into state strategies. **Cyberespionage targeting EU Member States and EU institutions remains persistent and continuous, with threat actors maintaining long-term access to networks, particularly in government, defence, and critical infrastructure sectors**. The convergence between state-sponsored actors and cybercriminal ecosystems has become more pronounced, with states leveraging criminal tools, access brokers, and shared infrastructures to enhance deniability and operational reach.

Within the cyber threat landscape, ransomware remains one of the most impactful threats, but its nature has continued to evolve. Attacks are now predominantly focused on data exfiltration and multi-layered extortion, rather than encryption alone. SMEs are increasingly targeted due to weaker security postures. While law enforcement actions disrupted major groups, the ecosystem has become more fragmented and adaptive, with a proliferation of new ransomware actors and rebranded operations. Critical sectors - including healthcare, transport, and public administration - continue to be heavily affected, with ransomware incidents maintaining a high share of impactful disruptions across the EU.

Supply chain attacks remain a key systemic risk, as attackers exploit dependencies on third-party providers and widely used software components to scale impact across multiple organisations. This risk is compounded by continued reliance on non-EU vendors and complex digital ecosystems, increasing exposure to vulnerabilities and external influence. Threat activity targeting cloud environments, managed services, and open-source software has expanded, reinforcing the potential for cascading effects. Together, these developments confirm a shift from isolated cyber incidents to a more interconnected, systemic, and strategically driven threat landscape. **Broader trends also point to growing pressure on cyber resilience, including a persistent cybersecurity skills gap** - still estimated in the hundreds of thousands across the EU - and ongoing challenges in public awareness and incident reporting.

At EU level, several laws and initiatives are in place to address some of these challenges, mitigate their impacts, or strengthen the level of cybersecurity across the Union. The proposal for a **Cybersecurity Act 2** (CSA2 proposal), adopted on 20 January 2026, clarifies and strengthens the mandate of the European Union Agency for Cybersecurity (ENISA); improves the European Cybersecurity Certification Framework (ECCF) and addresses ICT supply chain security challenges. Specifically, with the trusted ICT supply chain framework, the proposal aims at de-risking the Union's critical ICT supply chains, starting with the electronic communications sector. Anchored in the ICT supply chain framework, the new ECCF will deliver trust for critical ICT technologies such as 5G and cloud.

The CSA2 proposal also aims to establish a mechanism to validate the skills and experience acquired by cybersecurity professionals against a common set of criteria, defined at European level, and implemented at national level. By developing a mechanism of European individual cybersecurity skills attestations, it will facilitate skills portability and support the single market by supporting the emergence of new

providers. The CSA2 proposal will have positive economic impacts by supporting cybersecurity professionals' mobility, reducing labour and skills shortages in cybersecurity. It will create a market of cybersecurity attestations that are easy to understand for employers and learners, tailored to the European Union labour market.

The **NIS2 Directive strengthens the cyber resilience of critical sectors in the EU by requiring essential and important entities in these sectors to take cybersecurity risk-management measures and to report significant incidents.** By ensuring organisational measures, such as supply chain security measures, the Directive improves the cybersecurity baseline and supports the continuity of services that are essential for the society. Moreover, the Directive requires Member States put in place national cybersecurity strategies and coordination structures, supporting Member States' overall cyber preparedness. At European level, the Directive creates cooperation networks (NIS Cooperation Group, CSIRTs Network and EU-CyCLONe), with the objective of promoting trust, confidence and cooperation between Member States. By creating an overarching framework for cybersecurity in critical sectors, the NIS2 Directive also supports the preparation of critical infrastructure sectors against emerging cybersecurity threats, such as cryptographically relevant quantum computers (CRQC).

Concerning the cybersecurity of specific critical sectors, the Commission has continued the implementation of the Action Plan on the cybersecurity of hospitals and healthcare providers, in cooperation with ENISA, the European Cybersecurity Competence Centre (ECCC) and Member States. The ECCC launched a call for proposals, allocating EUR 30 million to reinforce cybersecurity capacities in hospitals and healthcare providers, while ENISA issued guidance on cybersecurity practices in September 2025. ENISA has set up a cybersecurity support centre for hospitals and healthcare providers, financed under a Contribution Agreement through the Digital Europe Programme. Building on these and other relevant actions, the Commission will put forward recommendations to further refine the Action Plan.

As regards the security of products with digital elements, the implementation of the Cyber Resilience Act (CRA) **will address insecure** hardware and software products circulating in the internal market and **being integrated** in ICT supply chains across sectors. Products lacking embedded cybersecurity requirements expand the risk surface of SMEs and critical infrastructure as they present exploitable vulnerabilities, creating risks of cascading disruptions and threats to the European economy and society, as showcased by the recent Collins Aerospace incident targeting airline check-in and boarding software. **Enforcing mandatory security-by-design and lifecycle obligations will improve Europe's cyber resilience and make cybersecurity a market differentiator rather than an afterthought**. Over time, the new EU cybersecurity regulatory framework will strengthen the EU's cybersecurity overall preparedness, reduce dependencies on high-risk third-country suppliers and position the EU as a global standard-setter in secure digital ecosystems.

Looking ahead, **future cybersecurity investment needs to build on what has already been achieved and focus on areas where strategic gaps remain.** Key priorities relate to Europe's preparedness, digital sovereignty, support regulatory implementation, and enable resilience in the face of accelerating threats and technological change. These priorities can be structured around three strategic investment pillars:

- Pillar 1 - Knowledge & R&I - This pillar strengthens Europe's technological foundations.
- Pillar 2 - Industrial scale-up & market uptake "Made in the EU" - This pillar consolidates a competitive European cybersecurity industry.
- Pillar 3 - Resilience of the Digital Market and Infrastructures - This pillar strengthens operational resilience.

Cybersecurity must also be treated as a cross-cutting priority. The resilience of digital infrastructures, public services and sectoral systems depends on ensuring that capabilities developed under dedicated cybersecurity programmes are consistently embedded across all investment areas.

Recommendation:

Member States should reinforce cybersecurity in critical sectors and across the digital value chain, by:

(i) taking measures to enhance cybersecurity in critical sectors commensurate to the level of risk, ensuring effective cooperation between relevant national authorities, as mandated by the NIS2 Directive, ensuring timely implementation of the Cyber Resilience Act, and engaging with the European Commission and the EU Agency for Cybersecurity (ENISA) on the new challenges posed by the cybersecurity capabilities of the most advanced AI models;

(ii) de-risking ICT supply chains based on Union-level coordinated security risk assessments, mitigating dependencies and phasing out high-risk suppliers from key ICT assets in critical infrastructure, including in electronic communications networks;

(iii) establishing structured multi-annual national funding mechanisms for cybersecurity, aligned with EU-level strategic priorities, to ensure the scale and continuity of investment required. Member States should allocate stable national funding envelopes dedicated to actions, such as the uptake of trusted European cybersecurity capabilities, the deployment of cybersecurity infrastructures, and the development of advanced cybersecurity solutions including dual-use, facilitating their access to later-stage capital. This coordinated investment effort should maximise the impact of Union programmes, reduce fragmentation, and provide the necessary critical mass to achieve strategic autonomy in key cybersecurity technologies. Similarly, strategic EU investment in AI cybersecurity capabilities and acceleration of adoption across strategic sectors will be critical to avoid a cyber offence-defence asymmetry in the near future;

(iv) continuing to develop the cybersecurity workforce by investing in skills on EU cross-border projects, and making use of the European Cybersecurity Skills Framework;

(v) putting in place measures to support the transition to Post -Quantum Cryptography in accordance with the timeline set in the Coordinated Implementation Roadmap for the Transition to Post Quantum Cryptography adopted in June 2025[68];

(vi) accelerating the actions foreseen in the Action Plan on cybersecurity of hospitals and healthcare providers, including the distribution of Cybersecurity Vouchers;

(vii) establishing robust and timely conformity assessment and supervision capabilities, providing targeted support - particularly to SMEs - to meet cybersecurity requirements, and fostering cross-border information sharing to strengthen product cybersecurity across the single market, notably in the context of the Cyber Resilience Act implementation;

(viii) developing sovereign, interoperable secure communications tools based on open-source protocols in line with the Preparedness Union Strategy, ProtectEU Strategy and the Council Recommendation for a Cyber Crisis Management Blueprint, to reinforce the EU's autonomy and strengthen the EU's ability to manage crises and ensure operational resilience.

3. Protecting and empowering people, reducing burdens and harnessing digitalisation for sustainability

Since its adoption in 2023, the European Declaration on Digital Rights and Principles has informed the Digital Decade Policy Programme, serving as an anchor of the digital transformation of the EU towards its human-centric vision. The principles support the Digital Decade's targets and guide actions in areas such as skills development, public services, solidarity and digital inclusion.

According to the Digital Decade Eurobarometer 2026, 51% of respondents consider that the EU protects their rights well in the digital environment. In addition, 85% of Europeans think the EU should cooperate with Member States to promote digital education and skills programs, while 84% think it is important that the EU fulfils the objective of ensuring that all EU citizens have basic digital skills (including AI literacy).

3.1. Digital skills for smart society and competitive economy

Empowering citizens and equipping workers with digital skills is at the core of Europe's digital transformation, in line with the Declaration on Digital Rights and Principles. Digital skills are both a social and an economic imperative. Basic digital skills are essential for meaningful participation in society, access to services, inclusion, and democratic resilience, while the availability of highly skilled professionals,

68 A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography | Shaping Europe's digital future

particularly ICT specialists, is critical to Europe's competitiveness, technological sovereignty, and capacity to deploy advanced digital technologies.

This section therefore addresses both dimensions. It first examines progress and remaining gaps in basic digital skills across the population, with particular attention to unequal access and evolving needs linked to AI and cybersecurity. It then assesses the EU's capacity to expand its pool of ICT specialists, a prerequisite for innovation, secure digital infrastructure and the wider uptake of advanced technologies across the economy.

In their National Roadmaps, Member States reported investments of EUR 24 billion in basic digital skills (8% of the total budget). The 349 measures reported on the roadmaps primarily focus on improving digital skills in formal education and promoting digital inclusion. This emphasis is also evident in Member States' roadmap adjustments.

For the training of ICT specialists, Member States reported investments of EUR 11.9 billion (4.1% of the total budget). The 208 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 focusing on those already in employment. This focus is also reflected in Member States' roadmap adjustments, which include a sharp increase in measures aimed at boosting advanced digital skills among women.

According to the European Declaration on Digital Rights and Principles, the digital transformation should contribute to a fair and inclusive society and economy that leaves nobody behind. It should benefit everyone, achieve gender balance, and include notably older people, people living in rural areas, persons with disabilities, or marginalised, vulnerable or disenfranchised people and those who act on their behalf. In this regard and according to the 2026 Eurobarometer on the Digital Decade, 90% of Europeans think it is important for the EU to make digital tools more accessible for everyone (especially vulnerable groups, older ones, people with disabilities, etc.). In addition, according to Eurostat, 24.9% of citizens across Europe use the internet for civic or political participation.

3.1.1. Basic digital skills

Over the last two years, the level of basic digital skills in the EU has increased significantly. The percentage of people with at least a basic level of digital skills rose by 4.8 percentage points, from 55.56% in 2023 to 60.39% in 2025. This represents a **year-on-year increase of 4.3%, significantly** higher than the yearly growth rate recorded between 2021 and 2023 (1.5%). Some Member States have made significant progress, with year-on-year increases of more than 6%, including Denmark, Romania, Ireland, Italy, Germany, Cyprus and Poland.

However, in 2025, the percentage of people with at least a basic level of digital skills still stood at only 92% of the ideal value of the Digital Decade trajectory (60.39% instead of 65.51%). According to the forecast along the updated baseline trajectory, only **85.6% of the target will be achieved by**

2030, implying that only 68.48% of the population is projected to have at least a basic level of digital skills, instead of the target of 80% (Figure 15).
At this pace of progress, it will take eight additional years from the digital decade deadline to reach the full target, forecast to be reached in **2037** if no further actions are taken.

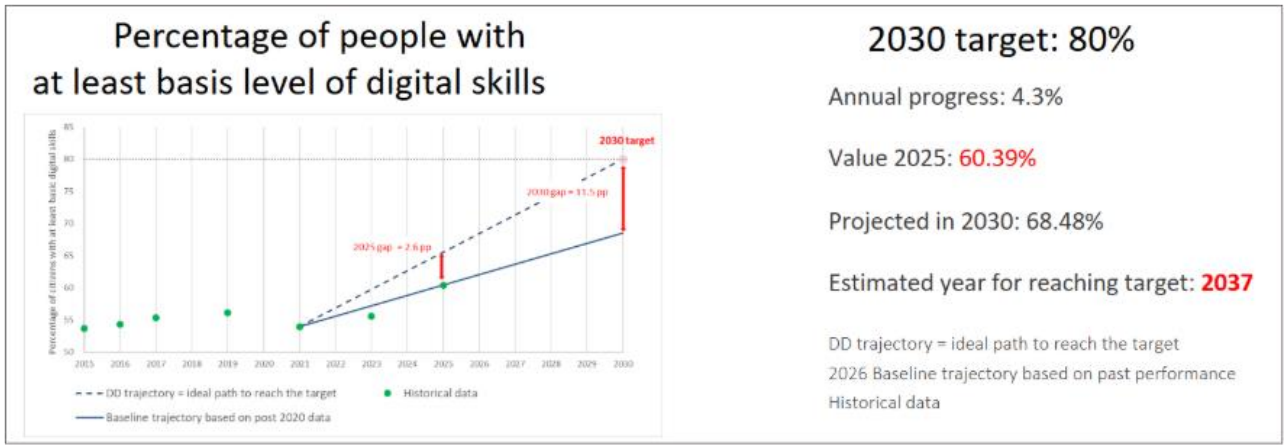


Figure 15: At least basic digital skills in the EU. Historical data, Digital Decade (DD) trajectory and revised baseline trajectory towards 2030.

Basic digital skills are essential for meaningful and safe participation in today's digital economy and society. As shown by the Eurobarometer on Future Needs in Digital Education (2025)[69], 89% of citizens agree that digital skills are essential for participation in society while more than eight in ten respondents (86%) agree that expanding digital skills training is important for improving the economy of their countries. Yet, a substantial share of Europeans still faces difficulties in acquiring them. Older people, individuals with low educational attainment, persons with disabilities, marginalised groups facing racial or ethnic discrimination, and those who are unemployed or outside the labour market remain particularly at risk of lacking basic digital skills. Disparities are also evident among younger generations: not all young people benefit equally from digital opportunities and factors such as unequal access to digital tools and infrastructure, as well as limited parental support, can significantly shape learning outcomes.

The barriers to acquiring digital skills go well beyond access to devices and internet connectivity. For older people the transition to new technological tools can be intimidating, especially where there is limited prior exposure, low confidence in using digital tools or a lack of age-appropriate training opportunities and guidance. People with lower educational attainment may face a double disadvantage: they may lack both foundational skills and the capacity for self-directed learning needed to improve their digital literacy. For those outside the labour market, digital upskilling may be deprioritised in favour of other skills perceived as more immediately relevant for re-entering employment. Language barriers can further restrict access when learning resources are not available in accessible formats or in learners' native languages. More broadly, the rapid pace of technological change means that digital skills need to be constantly updated, a

[69] European Union, Future Needs in Digital Education, Eurobarometer Survey, 2024.

task that requires time and resources that many individuals may not have. Under the **Union of Skills,** Member States are encouraged to strengthen basic skills provided in formal education and expand training opportunities and participation in lifelong learning. The STEM Education Strategic Plan [70] highlights the importance of increasing the talent pipeline in STEM subjects, and among its actions proposes a 5% enrolment target in doctoral programmes in ICT by 2030. The need to address skills shortages in strategic sectors, including ICT and AI, is also reflected in the Council Recommendation on Human Capital[71]. The Commission plans to adopt an education package, which will complement the Action Plan on Basic Skills and the STEM Education Strategic Plan and will aim to establish a robust and inclusive EU digital education ecosystem, which will help Member States support children and young people who struggle with digital skills. Furthermore, the EU-OECD AI literacy framework for primary and secondary education will put forward a common approach to the competences young people need to develop already at school to understand and critically use AI.

Particular attention should be paid to the evolving nature of digital skills needs. The acceleration of AI uptake is changing the skills profile required for full participation in society and the economy. People face increasing concerns over the protection of their sensitive data, as well as the need to securely interact with AI-based tools and services[72]. Education and training systems therefore need to adapt not only to persistent gaps in basic digital skills, but also to new demands related to AI literacy and cybersecurity awareness. This challenge is especially acute for disadvantaged groups, including people with low socio-economic backgrounds, those living in remote areas, older people, persons with disabilities, and adults outside the labour market, who often need more accessible, targeted and flexible learning pathways. It also requires strengthening the capacity of education and training systems, including teachers, trainers and local providers, to respond to changing skills needs in an inclusive and effective way.

Recommendation:

In line with the Digital Education Action Plan, Basic Skills Action Plan, the Apply AI Strategy, the STEM Education Strategic Plan, and the Council Recommendations on key enabling factors for digital education and training, improving the provision of digital skills and competences in education and training, and on human capital in the EU, Member States should prioritise coherent investments and policies to support digital education and skills, including:

(i) targeted policies and support for the most disadvantaged groups, including but not limited to people from low socio-economic backgrounds, those living in remote areas, those outside the

[70] European Commission, A STEM Education Strategic Plan: Skills for Competitiveness and Innovation, COM(2025) 89 final, 5 March 2025.

[71] Council of the European Union, Council Recommendation of 9 March 2026 on Human Capital in the European Union, 9 March 2026; Commission Regulation (EU) 2022/720 of 10 May 2022 on the Application of Article 101(3) of the Treaty on the Functioning of the European Union to Categories of Vertical Agreements and Concerted Practices.

[72] Eurobarometer on future needs in digital education (2025): the vast majority of respondents (85%) believes that digital skills are necessary to use generative AI tools safely and responsibly. A bit less than two-thirds (63%) of Europeans agree that everyone will need to be AI literate in 2030. This is particularly noticeable among younger people (66%-67% of aged 15-24 or 25-39 vs 62% of older age groups) and those still in education (75%).

labour market, older people and persons with disabilities marginalised groups facing racial or ethnic discrimination, as well as those insufficiently supported by formal education and workforce-based training;

(ii) actions to strengthen digital and AI literacy and basic cybersecurity skills across the population, including through regular assessment and tailored education and training.

3.1.2. ICT Specialists

The total number of ICT specialists in employment rose by 260 000, from 10.2 million in 2024 to around 10.5 million in 2025. **This reflects a 2.6% year-on-year growth in the number of employed ICT specialists**. In 2025, ICT specialists still accounted for just 5.0% of total EU employment, substantially stable since the previous year and far from the EU target of 10% of total employment by 2030.

According to the baseline trajectory, around 12.2 million ICT specialists are expected to be employed by 2030, meaning that only **61% of the target will be achieved by 2030** (Figure 16). **In 2025, the value reached by this KPI stood at around 78% of the ideal trajectory value,** with around 10.5 instead of 13.4 million. The full target - 20 million ICT specialists in employment by 2030 - is forecast to be reached only in **2052** if no further actions are taken.

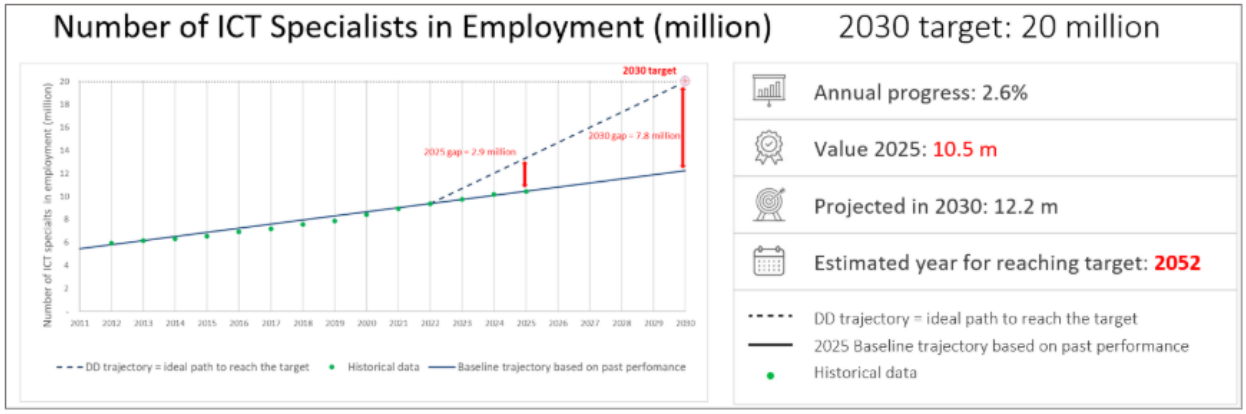


Figure 16: ICT specialists in the EU. Historical data, Digital Decade (DD) trajectory and revised baseline trajectory towards 2030.

In 2025, women accounted for 19.5% of employed ICT specialists, a figure unchanged since 2024. Over the past decade, the gender gap in ICT employment has remained pronounced, with **men consistently outnumbering women by around 60 percentage points**-women's representation fluctuated between 16.2% and 19.5%, while men's ranged from 80.5% to 83.8% (Figure 17).

Despite a **brief decline between 2013 and 2015**, the share of women in ICT roles has **grown gradually since 2012**, albeit at a slow pace (Figure 17, left). In contrast, the proportion of men peaked in **2014-2015** and has since declined, yet it still **exceeds women's representation by more than fourfold** (Figure 17, right).

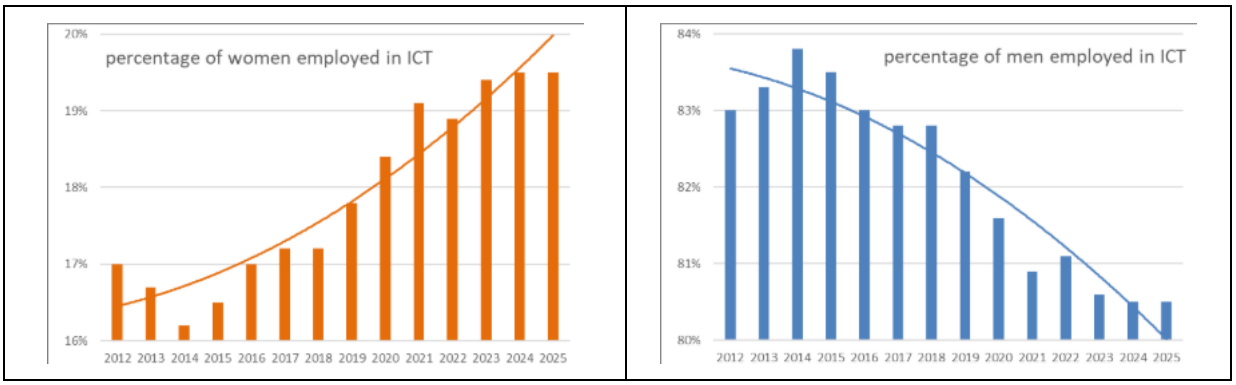


Figure 17: Percentage of individuals employed in ICT specialists' occupations in the EU by sex (2012-2025). The solid line shows the time trend since 2012. Left-hand side: percentage of women in total ICT specialists; right-hand side: percentage of men in total ICT specialists. Please note that the range of the y-axis is different in the two charts.

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.

The analysis of Online Job Advertisements (OJA)[73] reveals rapid shifts in specific skill requirements. Demand remains strongest for Data Science and Cybersecurity profiles, while cloud security skills are also rising significantly. The successful deployment of AI requires a complex mix of expertise in data management, cybersecurity, systems engineering and software development.

The rapid uptake of digital technologies across sectors, combined with replacement demand linked to retirement will put further pressure on the ICT workforce in the coming years. Shortages and mismatches are unevenly distributed across Member States, regions, sectors and firms, with stronger digital ecosystems generally better placed to attract and retain talent. Combined with the persistently low share of women among ICT specialists, this means that the European economy is still not making full use of its available talent base.

A number of **structural challenges** help explain this gap:

- There is a considerable mismatch of ICT skills in the European labour market. Many companies report difficulties in finding people with the required profile, a challenge made harder by rapidly changing skills demands linked to AI, the evolving data economy, and growing cybersecurity needs.
- There are key drop-off points (*'leaky pipeline'*) for girls and women in ICT fields notably between secondary STEM education and specialised ICT studies, and between ICT qualifications and employment. This suggests that increasing girls' participation in STEM alone will not be sufficient to close the gender gap. Evidence points to persistent barriers for women in the ICT workplace ('*leaky pipeline after entry*'), including gender bias in recruitment and promotion, unequal recognition and

[73] ZENODO, LEADSx2030 Advanced Digital Skills State-of-Play report, November 2025.

pay, limited access to leadership roles, and greater caregiving responsibilities leading to more frequent career breaks.

- The relatively low number of new ICT graduates (tertiary and initial VET) entering the labour market presents a major challenge to reach the Digital Decade target. In 2023, the EU produced only 2.7 tertiary ICT graduates per 1 000 young people, compared to 3.7 in the US and 4.6 in the UK. Although Member States are seeking to adapt Higher Education Programmes to changing skills demands and increase the attractiveness of ICT careers, current efforts remain insufficient.
- Another challenge lies in the upskilling of existing ICT specialists. Businesses must ensure that their employees remain up to date with the latest ICT skills requirements, which requires substantial investment. In addition, a growing number of sector specialists such as healthcare professionals using AI-powered screening tools, need advanced digital skills to use digital technologies effectively. This increases competition for talent and calls for more dedicated approaches to ICT education, enabling workers with non-technical backgrounds to interact efficiently and safely with advanced digital technologies.
- The concentration of the ICT ecosystem around individual vendors also presents considerable challenges for upskilling and reskilling. As technologies become increasingly vendor-specific, professionals are often required to obtain specialised skills and certifications tailored to particular applications or platforms. Such dependencies may reduce the portability of skills across employers and technologies, make training pathways more fragmented and costly and weaken workforce adaptability and resilience.

Addressing these challenges will require stronger investment in the development and updating of education and training provision, particularly in cooperation with Industry, as well as more flexible learning pathways and netter translation of research outcomes into practical training content. It will also require stronger efforts towards attract and retain women in ICT studies and careers, more support for workforce and in-company upskilling and greater attention to the territorial and sectoral distribution of ICT talent, so that regions and smaller firms are not left behind.

Recommendation:

In line with the STEM Education Strategic Plan, the Council Recommendation on human capital, the Council Conclusions on European Competitiveness in the Digital Decade and the AI Continent Action Plan, Member States should support the expansion of the ICT workforce by:

(i) supporting early exposure of young people, particularly girls, to STEM education, and promoting access of women to ICT careers throughout the entire education and career pathway;

(ii) promoting VET and lifelong learning in ICT and accelerating education and training course development in collaboration with industry, in particular through promoting and contributing to the EU Digital Skills Academies;

(iii) expanding labour migration pathways to attract highly skilled ICT specialists from non-EU countries and incentivising the return of European ICT talent.

3.1.3. Protecting people, in particular minors, in the online space

Protecting citizens, in particular minors, from harmful and misleading content online remains one of the most pressing challenges of the digital age. In 2025, 55.9% of EU citizens aged 16-74 declared having been exposed to untrue or doubtful content online, an increase from 49.25% since 2023. This corresponds to an annual growth rate of 6.5 percentage points. This trend is also observed in the younger population, with 61.66% of individuals aged 16 to 24 exposed in 2023, increasing to 66.34% in 2025, reflecting an annual growth rate of 3.7 percentage points. There is a notable gap favouring young people, with a difference of 7.77 percentage points between those aged 16-24 and those aged 25-64. For the latter group, the exposure increased from 51.7% in 2023 to 58.57% in 2025, with an annual growth rate of 6.4 percentage points.

Turning to online verification of information, the European Union saw an increase from 24.29% in 2023 to 29.16% in 2025 for all individuals aged 16-74, indicating an annual growth rate of 9.6 percentage points. Among individuals aged 16 to 24, the percentage increased from 34.68% in 2023 to 39.49% in 2025, with an annual growth rate of 6.7 percentage points. The gap between young people and those aged 25-64 is 9.09 percentage points. For individuals aged 25 to 64, the percentage rose from 25.18% in 2023 to 30.4% in 2025, with an annual growth rate of 9.9 percentage points.

Regarding online exposure to hostile or degrading messages, the European Union experienced an increase from 33.5% in 2023 to 39.72% in 2025 for all individuals aged 16-74, reflecting an annual growth rate of 8.9 percentage points. For those aged 16 to 24, the exposure increased from 47.54% in 2023 to 52.99% in 2025, with an annual growth rate of 5.6 percentage points. The gap between young people and those aged 25-64 is 11.85 percentage points. For individuals aged 25 to 64, the exposure rose from 34.53% in 2023 to 41.14% in 2025, with an annual growth rate of 9.2 percentage points.

In summary, the data from the Eurostat surveys reveals a consistent increase in online exposure to both untrue or doubtful content and hostile or degrading messages among EU citizens from 2023 to 2025, with younger individuals particularly at risk. Encouragingly, this is accompanied by an increase in the practice of information verification, again most pronounced among younger individuals. While these trends suggest a growing awareness of online risks, the overall picture underlines the need for policymakers to enhance digital literacy programmes and strengthen measures to protect EU citizens in the digital space. The significant gaps between age groups should be considered when designing targeted interventions.

Preserving information integrity

With the digitalisation of the information space, citizens increasingly face challenges in accessing a plurality of information from independent and reliable sources. The 2025 Media Pluralism Monitor shows that there is a **medium to high risk to media pluralism in 23 EU Member States.** Additionally, online

platforms and AI services increasingly capture news revenues, putting the news sector under significant economic pressure, ultimately threatening media independence and pluralism. This shows the need to strengthen financing mechanisms for news media, in ways that respect media independence, as well as to support news organisations in better harnessing new technological tools.

To counter the escalating threats of disinformation, foreign interference, and algorithmic amplification of harmful content, evidenced by the 6.5 percentage-point annual increase in exposure to untrue or doubtful content (2023-2025) and the growing fragmentation of media pluralism, Member States must fully utilise the EU's existing legislative framework and non-binding instruments. These include the Digital Services Act (DSA), the Political Advertising Regulation, the AI Act, and the European Media Freedom Act (EMFA), as well as the voluntary Code of Conduct on Disinformation, which taken together form a cornerstone for systemic resilience. Several measures under the European Democracy Shield (EDS) as well as the EDMO Hubs provide important supportive frameworks, which complement efforts to ensure rigorous, coordinated enforcement of relevant EU legislative frameworks, both at EU and national levels.

Generative AI represents another evolving challenge. According to the latest Eurostat data, there is substantial uptake of generative AI tools, especially by the younger demographic. In 2025, 63.8% of young people aged 16-24 in the EU used generative artificial intelligence (AI) tools compared to just 32.7% of those aged 16-72. Reports have shown that foreign powers have been trying to poison LLM training data through techniques such as AI grooming (one example of this is Russia's Pravda network). Together with other problems noted in AI chatbots such as hallucinations or sycophancy, this creates a risk of untrue or doubtful content or even manipulation especially for the younger segment of the population.

Protecting children

According to the 2026 Digital Decade Eurobarometer survey, **an overwhelming majority of respondents (93%) think it should be a high priority for the EU to further strengthen the protection of children and young people online.**

With growing public concern over the risks children face in digital spaces, it is important to continue enhancing their online safety and well-being through robust regulatory and enforcement measures. In response to the demands by citizens, the Commission has been working on several streams to increase the well-being and safety of children online.

The **General Data Protection Regulation (GDPR)** already recognises that children merit specific protection regarding the processing of their personal data. Accordingly, organisations must implement child-specific data protection measures to provide a higher level of protection against the risks that may arise from children's use of digital services. The GDPR also contains specific safeguards for minors, including the 'right to be forgotten', and establishes age-of-consent requirements for the processing of personal data by information society services, such as social media, online gaming and other digital platforms.

Further reinforcing these protections, **Article 28 of the Digital Services Act (DSA)** requires providers of online platforms of all sizes accessible to minors to ensure a high level of privacy, safety and security for

minors on their services. To further boost online safety for children and young people under the DSA, the Commission adopted the **Guidelines on the protection of minors** in 2025. These guidelines set out a benchmark that the Commission uses to determine compliance in this area and outlines a non-exhaustive list of proportionate and appropriate measures to protect children from online risks such as grooming, harmful content, problematic and addictive behaviours, as well as cyberbullying and harmful commercial practices that may occur on online platforms accessible to minors. First enforcement actions have been taken against the providers of TikTok, Facebook and Instagram as well as pornographic-content online platforms. These investigations concern issues such as accessing age-inappropriate content, addictive behaviour, account settings and appropriate age assurance methods. Additionally, Digital Services Coordinators (DSCs) have started to enforce Article 28 of the DSA at the national level [74].

To strengthen protection for young audiences in an evolving digital landscape, the Audiovisual Media Services Directive (AVMSD) imposes obligations on video sharing platforms providers to embed EU content standards and child-safeguarding measures into their operations. Under the AVMSD, all video-sharing platforms (VSPs) must include EU media content standards, notably those aimed at protecting minors from harmful content, in their terms and conditions. Their providers are also required to take appropriate measures (e.g. mechanisms to report or flag harmful content, age verification, parental control and content rating systems) to prevent minors from viewing harmful content. The Commission continues to monitor the implementation of the AVMSD by the Member States, including the provisions pertaining to the protection of minors. In addition, the Directive's ongoing evaluation and review planned by Q3 2026 will assess whether more should be done to ensure that minors are protected when they view audiovisual content online, including when made available by influencers when they qualify as audiovisual media service providers.

In response to the growing epidemic of cyberbullying[75] the Commission has adopted an action plan against cyberbullying[76]. The initiative aims to strengthen the capacity to prevent, report and combat cyberbullying. The plan was prepared through targeted and public consultations involving children, researchers, experts, and the wider public.

The action plan is structured around three pillars:

- **A coordinated EU approach to protection:** The Commission will enforce existing laws while strengthening their focus on cyberbullying and invites Member States to develop national policies based on a shared understanding of the issue.

[74] Authority for Consumers and Markets, ACM launces DSA investigation into Snapchat in connection with illegal sale of vaping products to minors, September 2025, and, Authority for Consumers and Markets, ACM launches investigation into Roblox in connection with risks that minors are facing, January 2026.

[75] Joint Research Centre, Cyberbullying: Insights from science, policy and legislation - Publications Office of the EU, 2025.

[76] European Commission, Action Plan against cyberbullying, February 2026.

- **Prevention and awareness:** The plan promotes responsible digital habits from an early age and will provide EU-level tools developed with input from key stakeholders.
- **Reporting and support:** The plan ensures clear and accessible reporting and support for all, especially victims and bystanders. The Commission will support the rollout of an online safety app across Member States to help children report cyberbullying, store evidence and access assistance.

Lastly, efforts to establish an EU-wide approach to age verification are advancing, with the release of the blueprint for a secure, privacy-preserving and fully data-protection-compliant **EU Age Verification solution** in July 2025. On 15 April 2026, the Commission presented the feature-complete EU age verification solution. In parallel, and to accelerate progress across the EU, the Commission adopted a recommendation on 29 April 2026 urging Member States to make use of the age verification blueprint and draw up implementation plans to ensure swift adoption of national age verification solutions by 31 December 2026. The forerunner Member States (DK, FR, GR, IT, ES, CY and IE) are advancing with their implementation of the Age Verification solution, and the first national solutions are expected to be available mid-2026.

Recommendation:

Member States should reinforce the protection of people and minors in the online space, by:

(i) strengthening national implementation and enforcement of the Digital Services Act, including with targeted strategies countering Foreign Information Manipulation and Interference (FIMI), drawing on the FIMI Toolbox to integrate cross-sectoral coordination, dedicate funds to research, fact-checking and media literacy initiatives, and implement secure information-sharing mechanisms;

(ii) Member States should reinforce the protection of people and minors in the online space by ensuring sufficient administrative capacity of the Digital Services Coordinators to effectively enforce the Digital Services Act;

(iii) implementing the harmonised privacy preserving EU age verification solution in the national EUDI Wallets or stand-alone applications, including systems for issuing proof-of-age attestations, and accelerating the issuance of electronic means of identification to minors;

(iv) implementing the action plan against cyberbullying through coordinated national approaches, prevention and awareness measures, and accessible reporting and support mechanisms;

(v) Member States should reinforce the protection of people and minors in the online space by ensuring sufficient administrative capacity of the Digital Services Coordinators to effectively enforce the Digital Services Act.

3.2. Efficient public services and administrative burden reduction

This section examines how the digital transformation of public services can improve efficiency, reduce administrative burden, and enhance accessibility for citizens and businesses across the Union. Building on

the Digital Decade principles, it focuses on key enablers such as secure digital identity, interoperable services, and access to essential public services online. While progress is ongoing, further efforts are needed to streamline procedures, strengthen cross-border functionality, and ensure that digital solutions deliver tangible simplification benefits.

The European Digital Rights framework requires all Member States to offer citizens an accessible, voluntary, secure and trusted digital identity. This should in turn allow people to access a range of online services, including medical records and other healthcare data. According to the Digital Decade Eurobarometer 2026, 79% of Europeans think EU should cooperate with Member States to develop shared digital public services (e.g. digital ID, e-Health).

3.2.1. European Digital Identity and business wallets

The European Digital Identity (EUDI) Framework is a key enabler of Digital Decade targets. Electronic identification[77] allows people to securely verify their identity and access services across the EU. According to 2025 data, 52% of people aged 16-74 in the EU stated that they had used their eID to access online services for private purposes in the previous 12 months. Results vary significantly across Member States, from over 90% in Denmark (99%), Finland (96%), the Netherlands (95%), Sweden (92%), and Estonia (91%) to below 15% in Germany (15%), Slovakia (14%) and Bulgaria (12%). Some countries are showing rapid progress, with Cyprus improving its score from above 9% (2024) to 57% (2025).

Under Regulation (EU) 2024/1183 establishing the European Digital Identity (EUDI) Framework, each Member State is required to provide an EU Digital Identity Wallet by the end of 2026. **All Member States are actively developing their European Digital Identity Wallets.**

The EU Digital Identity Wallets build on the national digital identity systems already in place in several Member States. The new regulatory framework expands the functionalities and usability of national eIDs and ensures their mutual recognition across the EU.

To ensure that EUDI Wallets are secure, each national EUDI Wallet must be **certified in accordance with the Cybersecurity Act** complemented by national certification schemes to ensure compliance with functional and data protection requirements, in full respect of the GDPR.

Building on the EU Digital Identity framework, in addition to several other tools (the Single Digital Gateway, the Once Only Technical System, the Digital Product Passport, the European Unique Identifier) European Business Wallets are expected to provide a single, trusted digital infrastructure that allows businesses to operate seamlessly across the EU by reducing administrative burden, simplifying compliance with EU legislation both in a B-2-B or B-2-G, increasing legal certainty, and enabling secure data exchange. European Business Wallets will help companies automate everyday time-consuming administrative tasks.

[77] Eurostat, Digitalisation Dashboard, accessed in May 2026.

Instead of repeatedly and manually filling in forms, sending documents, or verifying information, businesses can reuse trusted data and complete processes automatically.

All limited liability companies registered in the EU have automatically been assigned a European Unique Identifier (EUID) since 2017. It will be assigned to all EU commercial partnerships by July 2028. The identifier allows, through a Business Registers Interconnection System (BRIS), public access to company information – including information on branches in other Member States – via the European e-Justice portal. The EUID is also used by the Beneficial Ownership Register Interconnection System (BORIS), where the EUID is assigned to all relevant entities, not only companies. In accordance with Directive 2025/25, BRIS will be linked with BORIS and the Insolvency Registers Interconnection System (IRI) by July 2028. The European Business Wallet will also use the EUID as a unique identifier contained in the Business Wallet owner identification data.

This means less back-and-forth, fewer errors, and faster execution - from onboarding partners to signing contracts or meeting compliance requirements. In practice, it frees up time and resources, allowing companies to turn compliance with EU legislation into competitive advantage and focus on growth instead of administration.

Recommendation:

Member States should ensure the timely deployment and uptake of the EU Digital Identity Wallet and prepare for the rollout of the European Business Wallet, by:

(i) ensuring the issuance of the Wallet by the December 2026 deadline and aligning national EUDI Wallets implementation roadmaps, including security certification and cross-border use cases;

(ii) supporting the integration of the Wallets with key public and private services and use cases, in order to maximise the uptake and the economic impact of the EUDI Wallets, building on the continuing work of the large-scale pilots.

3.2.2. Digital Public Services for Citizens and businesses

In 2025, the EU made steady progress towards its Digital Decade targets for fully digital public services. The digital public service score for citizens rose by 2.3 points, from 82.3/100 in 2024 to 84.6/100 in 2025. This represents a **year-on-year growth rate of 2.8%**.

According to the forecast along the baseline trajectory, **92.3% of the target is expected to be achieved by 2030** (Figure 18). **In 2025, the score for citizens stood at about 87.6% of the ideal value along the Digital Decade trajectory** (84.6/100 instead of 96.6/100). However, the full target - a score of 100 corresponding to the process fully online for all the services - is forecast to be reached only in **2058** if no further actions are taken. **The score of cross-border online availability stood at 75.3/100 in 2025, up from 71.3/100 in 2024, representing a year-on-year growth rate of 5.6% and reflecting continued progress.**

In their National Roadmaps, Member States reported investing EUR 13.9 billion, representing approximately 4.8% of the total budget, to drive the digitalisation of key public services. This investment included a comprehensive set of 307 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.

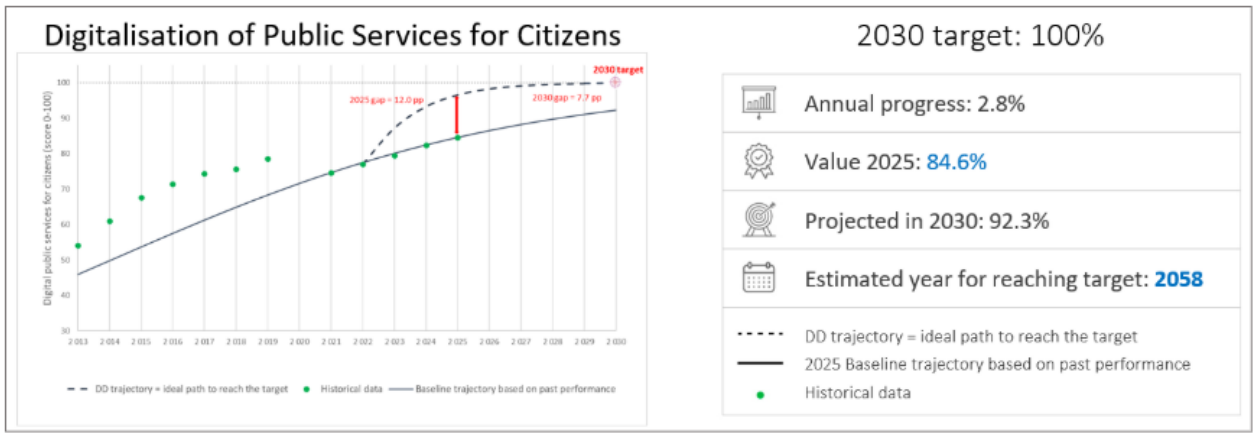


Figure 18: Share of administrative steps that can be done online for major life events for citizens nationals and foreigners (0 = no steps can be done online; 100 = the whole process can be done online). Historical data, Digital Decade and revised baseline trajectory.

The digital public service score for businesses rose by 2.4 points, from 86.2/100 in 2024 to 88.6/100 in 2025. This represents a **year-on-year growth rate of 2.7%**.

According to the forecast along the baseline trajectory, **93.7% of the target is expected to be achieved by 2030** (Figure 19). **In 2025, the score for businesses stood at 91% of the ideal value along the Digital Decade trajectory (88.6/100 instead of 97.4/100)**. However, the full target, a score of 100 corresponding to the process fully online for all the services, is forecast to be reached not earlier than **2063** if no further actions are taken. **The score of cross-border online availability stood at 78.4/100 in 2025, up from 73.8/100 in 2024, representing approximately a year-on-year growth rate of 6.2%**.

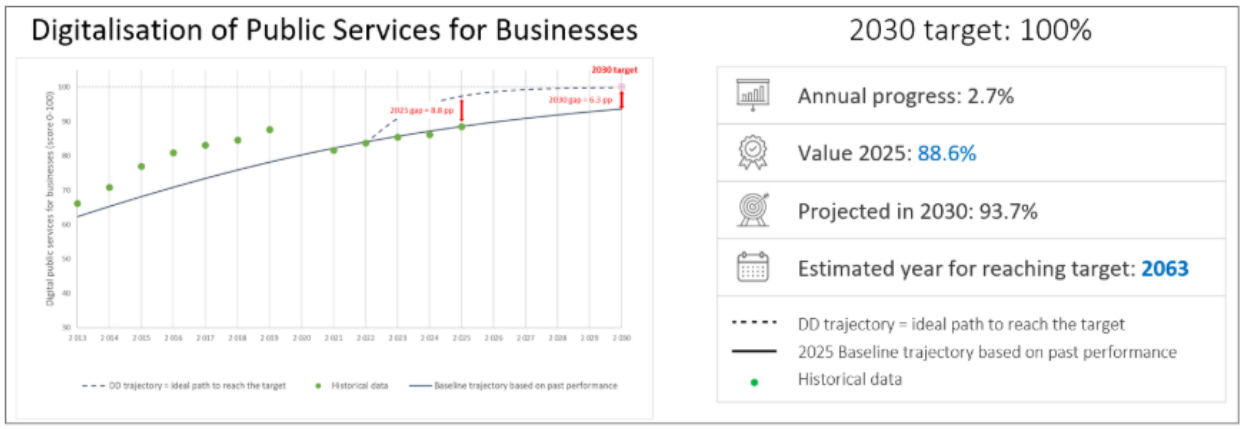


Figure 19: Share of public services needed to start a business and conduct regular business operations that are available online for national and for foreign users (0 = no steps can be done online; 100 = the whole process can be done online). Historical data, Digital Decade and revised baseline trajectory.

Member States, supported by a comprehensive EU policy framework, have undertaken significant actions to develop secure, interoperable and user-centric digital public services. These collective efforts have led to measurable improvements in availability and usability across the Union. However, implementation remains uneven, with persistent gaps in cross-border service provision, interoperability in practice, and emerging challenges related to security, advanced technologies and digital sovereignty. In addition, territorial evidence highlights that the effectiveness of digital public services depends not only on their availability but also on their accessibility, usability and integration into local contexts, which can vary significantly within Member States[78].

This is particularly important given emerging evidence that increasing digitalisation risks creating unequal access to public services. While 68% of EU residents interacted digitally with public authorities in 2025, significant disparities exist. According to Eurostat, there is a gap of 21 percentage points between 25–64 and 65–74 years old, and highly educated individuals are twice as likely to interact digitally with public authorities as those with low educational attainment. Additionally, Eurofound[79] research warns that digital-by-default approaches can disadvantage those with lower digital skills, limited internet access, disabilities, or complex needs. Member States have stressed the need for accessible and inclusive service delivery models to avoid reinforcing existing inequalities[80].**Cross-border service provision remains the main structural bottleneck**. Despite progress, a substantial number of services still require further development to meet Digital Decade targets. Key sectors affecting mobility, in particular health and justice (for example, starting a small claims procedure) still struggle to provide fully online cross-border services

[78] ESPON, DigiReg – Territorial Perspectives of Digital Transition in European Regions, 2024.
[79] Eurofound (2025), https://www.eurofound.europa.eu/en/publications/all/digitalisation-social-protection
[80] https://op.europa.eu/en/publication-detail/-/publication/56969910-beba-11f0-a612-01aa75ed71a1/language-en

for citizens. Beyond small claims, digitalisation of other cross-border judicial proceedings is underway, but implementation is costly and takes time. Similarly, digitalising permits, official business certificates and proof documentation remain most complex for businesses operating cross-border. This reflects the fact that, while interoperability frameworks are well established at EU level, their implementation across administrations is still ongoing. Core components, including cross-border data exchange and the once-only principle, are not yet fully operational in practice and not implemented in all policy domains of the public sector. In particular, the operationalisation of the once-only principle through the Once-Only Technical System (OOTS) remains incomplete, with many authorities not yet fully connected. In addition, while Member States increasingly rely on external providers for the development and delivery of digital public services, public procurement is not yet systematically leveraged to steer the development and uptake of secure, interoperable and sovereign digital solutions. A significant progress is expected under Directive 2025/25 on upgrading the use of digital tools and processes in company law. This will allow companies to obtain an EU Company Certificate from national business registers or through the system of interconnection of registers (BRIS) for different purposes, including in administrative procedures before national authorities or Union institutions and bodies, and in judicial proceedings in other Member States. The EU Company Certificate will be issued and certified by national business registers and will include essential information used by companies in cross-border situations, such as the company name, its registered office, legal representatives or the object of the company. The electronic EU Company Certificate will be authenticated by using trust services as referred to in Regulation (EU) No 910/2014 of the European Parliament and of the Council. Company law acquis already provides for online formation, registration and filing procedures, relying on the interconnection of business registers and covering cross-borders corporate reorganisation operations (conversions, mergers, divisions). The proposal for a Regulation on the 28th regime corporate legal framework 'EU Inc.' significantly streamlines cross-border scaling-up through fully digital procedures accessible through the Business Wallets, and the development of an EU central interface, based on the BRIS infrastructure.

Progress in local digital capabilities is currently foundational but limited, consisting mainly of isolated pilots in cities. Although Member States and local and regional authorities are increasingly investing in data-driven governance, these efforts remain largely fragmented and project-based, with limited cross-border coordination. However, the transition from these experiments to large-scale, reusable digital solutions is now being enabled through newly established legal and governance structures, notably the **Local Digital Twin (LDT) CitiVERSE EDIC**. Involving 15 Member States, this consortium focuses on scaling up advanced, AI-based urban planning simulations and generative AI, VR/XR applications to improve citizen interaction, establishing a common infrastructure that directly supports the cross-border reuse of proven digital public services across European cities.

Other EU-level instruments, including the Interoperable Europe Act, the Single Digital Gateway Regulation and the European Digital Identity framework, provide additional foundation for cross-

border data exchange and authentication. Their effectiveness, however, depends on sustained and coordinated implementation by Member States.

Progress is also visible in enabling functionalities and user experience, notably through the increased use of pre-filled forms to reduce administrative burden and the continued high performance of user support and mobile-friendly services.

Common challenges persist in security, sovereignty and the uptake of advanced technologies. While improvements have been recorded, uneven compliance with security controls and secure Internet standards across public sector websites indicates the need for further efforts to strengthen trust and readiness to face an evolving threat landscape. In parallel, reliance on non-EU network operators for the hosting and network-level delivery of government websites and email services raises shared concerns regarding digital sovereignty and long-term resilience. This underlines the need for a more strategic approach to the development and deployment of sovereign digital solutions within the public sector, including through choices made in service design, infrastructure and procurement.

Finally, while Member States are exploring artificial intelligence in public service delivery, including through chatbots for user support, its deployment remains at an early stage, limiting its impact on efficiency and user experience.

Overall, Member States have made steady progress, but achieving fully interoperable, secure and sovereign cross-border digital public services by 2030 will require sustained and coordinated collective action across the Union.

Recommendation:

Member States should step up coordinated investments and regulatory measures to develop and deploy secure, sovereign and interoperable digital solutions for online public and government services, including:

(i) accelerating the connection of competent authorities to the Once-Only Technical System (OOTS) and the full implementation of the Single Digital Gateway Regulation;
(ii) making more systematic use of public procurement to support the development and uptake of secure and sovereign digital solutions across the Union;
(iii) strengthening the cross-border dimension of public services through the Interoperable Europe Act framework and engagement with the IMPACTS-EDIC.
(iv) engaging with multi-country initiatives, as the LDT CitiVERSE EDIC, to enable their cities and regions to deploy AI-driven urban solutions and leverage reusable cross-border services.

3.2.3. e-Health

The conceptual framework of the e-Health indicator is focused on the availability of electronic health data for European citizens and does not measure actual usage of online health data access services. The

framework consists of four thematic dimensions, each including indicators that measure key aspects of the availability of online access to electronic health record data. In total, there are 12 sub-indicators in total at country level that describe:

1. the nationwide availability of online access to electronic health data;
2. the categories of accessible health data;
3. the availability of authentication schemes, type of front-end solutions and their coverage;
4. accessibility for certain categories of people, including vulnerable groups.

The composite e-Health indicator is an aggregate measure of the scores of each thematic dimension calculated as an average of the 12 sub-indicators.

The baseline trajectory is estimated on the basis of the three available data points, from 2022 to 2025. The observed points are well above the ideal path connecting the e-Health indicator value at the start of the programme with its EU target value (100/100) (Figure 20). **The access to eHealth indicator rose by 3.8 points, from 82.7 in 2024 to 86.5 in 2025.** This represents a year-on-year increase of **4.6%.** According to the forecast along the baseline trajectory**, the target is expected to be achieved by 2028** (Figure 20).

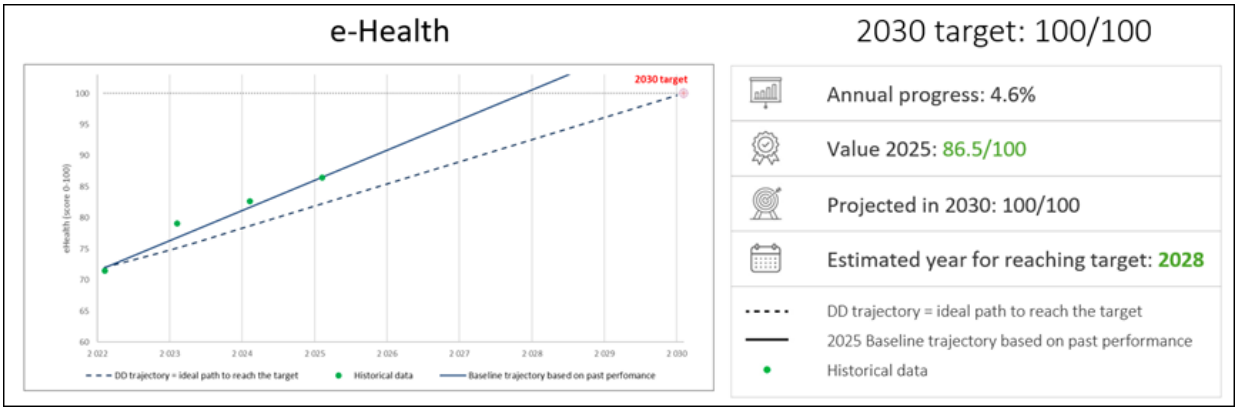


Figure 20: e-Health composite indicator. Historical data, Digital Decade and revised baseline trajectory.

Accelerating the digitisation of health systems to improve access to and sharing of electronic health records (EHRs) is crucial for boosting **EU competitiveness and technological sovereignty**[81]. EU Member States are taking significant steps in this direction by setting up public services to facilitate access to health data for primary and secondary use as mandated under the European Health Data Space (EHDS) Regulation. By leveraging a strong regulatory framework, collaborative resource pooling, advanced data infrastructures, and high-performance computing facilities, health data can be harnessed to develop the next generation of **European AI models** for personalised disease prevention and precision medicine.

[81] European Commission, The future of European competitiveness: Report by Mario Draghi, September 2024,

These solutions have the potential to address rising healthcare costs by promoting **simplification and efficiency**, ultimately leading to better outcomes for citizens.

According to the OECD's live repository of AI strategies & policies, at least 19 EU Member States recognise health as a crucial sector in their national AI strategies or related initiatives. However, AI adoption and integration in healthcare across the EU remain limited and uneven. Although 94% of EU healthcare providers are already using or planning to invest in AI within the next four years, challenges persist in scaling up investment and integrating advanced technology into often under-resourced healthcare systems[82].

In their National Roadmaps, Member States reported investing EUR 7.7 billion to support e-Health services (all coming from public budgets), with approximately 98 measures, most of them focusing on accessibility and uptake.

Addressing these issues requires targeted policy measures at national and European levels. The Commission announced in the **Apply AI Strategy** four flagship initiatives to boost AI adoption in healthcare and pharmaceuticals. The network of European AI-powered advanced screening centres will speed up the introduction of innovative solutions for prevention, early detection and diagnosis in cancer and cardiovascular diseases, while the European Network of Expertise on AI Deployment in Healthcare will consolidate guidelines and best practices to safely and effectively integrate AI in healthcare settings.

EU Member States are progressing towards achieving universal citizen access to their EHRs by 2030, as indicated by this year's **e-Health indicator**. Efforts are also ongoing to ensure that national, regional and local health information systems are operational by March 2029 for health data to be processed in line with the EHDS Regulation. This will provide robust governance and accelerate the implementation of necessary infrastructures, ensuring continuity of care by connecting various providers, and enhancing accessibility of health data for citizens and other authorised users. Moreover, mature health information systems will support the deployment of AI solutions by enabling the safeguarded secondary use of anonymised or pseudonymised health records.

However, progress remains uneven across Member States, reflecting differences in administrative capacity, digital maturity, and investment levels. Insufficient funding, digital skills and readiness among healthcare professionals, as well as inconsistencies in data quality and harmonisation across healthcare providers limit interoperability and information exchange within and across health systems. The EHDS Regulation provides an opportunity to address these issues. It mandates the establishment of Digital

[82] European Commission, PwC, EEIG, Open Evidence, Study on the deployment of AI in healthcare, 2025.

Health Authorities and health data access services for primary use, as well as Health Data Access Bodies for secondary use by March 2027[83].

Finally, European initiatives are paving the way for the cross-border harmonisation, secure storage, processing and analysis of health data for high-impact use cases, such as genomics and imaging-AI. The Genomic Data Infrastructure (GDI) and Cancer Image Europe platform (EUCAIM) projects are developing federated infrastructures and governance which aim to support and complement the implementation of the EHDS. In GDI, more than half of EU Member States are expected to have operational federated infrastructures by late 2026, advancing towards a secure and decentralised access to genomic and clinical data across Europe. The Cancer Image Europe Platform already supports the optimisation of the use of medical imaging and AI for personalised cancer care offering over 80 medical imaging datasets, preprocessing tools, and capabilities for distributed AI algorithm training.

Building on the above, **new investments in the digitalisation of health systems to facilitate the adoption and integration of AI in healthcare are needed.** This involves leveraging the EHDS and secure federated health data infrastructures to ensure safe storage, processing, and analysis of health data, as well as enhancing the digital skills and readiness of healthcare professionals.

Recommendation:

Member States should continue to cooperate and invest in the digitalisation of healthcare systems to strengthen the EU's competitiveness and strategic sovereignty while improving health outcomes for citizens, by:

(i) establishing the necessary public services and health information systems to enable universal citizen access to their electronic health records and to facilitate secure access to health data for secondary use, in line with the EHDS Regulation;

(ii) advancing the development and deployment of safe, trustworthy AI in healthcare by developing and implementing national strategies and roadmaps with monitoring frameworks;

(iii) accelerating cooperation on European health data infrastructures through EDICs and supporting the participation of healthcare organisations in the activities of the Apply AI Strategy's Network of AI-powered Advanced Medical Centres.

[83] Primary use of data means using electronic health data, to treat or rehabilitate patients, prescribe or dispense medical products and deliver associated social, administrative, or reimbursement services. In contrast, 'secondary' use refers to reusing existing data that was collected during primary use for scientific research purposes, public interest, policy support.

3.3. Digital for decarbonisation and sustainable technologies

Digitalisation can help decarbonise and make Europe's economy more resource efficient, but these benefits are not automatic. They depend on whether digital solutions deliver a measurable net positive impact and whether the expansion of digital infrastructures remains compatible with energy, water and material constraints. This section therefore looks at both sides of the equation: digital for sustainability, and the sustainability of digital itself. When citizens were asked about the synergies between digital and green transitions in the Digital Decade Eurobarometer 2026, 50% of them positioned the green digital technologies (e.g. energy-saving tech) between the technologies that will have the most positive impact on their daily life in the next 10 years. In addition, 78% of respondents think AI should be developed as a priority in an environmentally sustainable way (e.g. using renewable and clean energy).

The revised Digital Decade National Roadmaps include 62 measures from 18 Member States contributing simultaneously to the Digital Decade's green and digital objectives. Of these 59 measures, 37 are specifically designed to simultaneously address those green and digital objectives, with a total investment of EUR 222.2 million.

3.3.1. Sustainable digitalisation for competitiveness, resilience and net positive impacts

Sustainability is no longer only an environmental objective. It is increasingly a driver of industrial growth, competitiveness, innovation and resilience. However, digital contribution to climate neutrality and circular economy (clean industry) is not automatic. It depends on achieving a measurable net positive climate impact and realising its potential in enabling circular, profitable and future proof business models.

A fundamental issue to ensuring such net positive impacts is the pacing problem: the speed of technological change in digital markets, particularly AI and compute infrastructures, often exceeds the speed of policy, permitting and reporting systems. This creates a growing need for faster monitoring, comparable sustainability metrics, and earlier coordination between digital, energy and environmental authorities.

The convergence of digital and green strategies can strengthen the EU's competitiveness, sovereignty and resilience while contributing to achieving climate goals. Enabling smart technologies and making digital infrastructure more environmentally friendly reduces operational costs and encourages consumer adoption. GreenTech development will depend heavily on digital capabilities such as connectivity, AI infrastructure, cloud-edge systems, semiconductors, interoperable data systems and circular digital hardware[84]. The digital layer enabling this transformation needs to be built, scaled and anchored in the

[84] There is no single internationally agreed definition of green technology. The UN broadly defines it as technology with "the potential to significantly improve environmental performance relative to other technologies." For the purposes of this report, green technology (or "greentech") refers to technologies, products, and systems that measurably reduce environmental harm,

EU, with the potential to optimise supply chains and creates profitable, circular business models. All these factors contribute to decarbonisation and strengthen Europe's position in the green technology sector.

The digital sector's "hidden" material footprint remains a primary threat to European strategic autonomy. The production of digital devices relies on significant volumes of raw materials, many of them not found in the EU, energy, water and complex global supply chains, increasing the EU's exposure to external dependencies and resource risks.

AI is increasingly acknowledged as a transformative force for the green transition. It can serve as a key enabler of system intelligence, improving renewable forecasting, grid balancing and predictive maintenance, and enabling flexible demand that adjusts to variable solar and wind output. AI-based fault detection can reduce outage durations by 30 to 50%, and remote sensors combined with AI-based management could unlock up to 175 GW of additional transmission capacity without any new lines being built, according to the IEA's Energy and AI report (2025)[85]. Much of AI's environmental footprint is concentrated in a relatively small number of large, power-intensive data centres, with a typical AI-focused facility consuming as much electricity as 100 000 households[86]. This dual reality makes transparent monitoring and proportionate governance increasingly important.

3.3.2. Rising environmental concerns: electricity, water and material demand for digital transition

Despite the promising benefits of digitalisation for the green transition, the environmental footprint of the digital economy is intensifying. In 2025, data centres in Europe consumed approximately 72 terawatt-hours (TWh) of electricity, compared to 70 TWh in 2024, highlighting the sector's substantial and rising energy requirements. By 2030, electricity usage by data centres in Europe is expected to rise towards 115 TWh, an increase by at least 45 TWh compared to 2025.[87] While data centres are major energy consumers, they also have the potential to enhance system flexibility and demand response. Under the right conditions, they can offer grid services through on-site battery storage, adaptable cooling systems, load shifting, or by transferring computing tasks from one region to another as a form of sustained curtailment.

Water use is also becoming more relevant, particularly in regions facing water stress. Data centre cooling technologies, site selection and reuse of waste heat and water should therefore be considered as part of sustainable infrastructure planning.

---

improve resource efficiency, and support a more sustainable economy - spanning both hardware (e.g. batteries, heat pumps, solar modules) and software (e.g. grid optimisation, climate analytics). The term lacks an officially adopted European Commission definition; the closest legislative equivalents at EU level are the EU Taxonomy for Sustainable Activities and the list of net-zero technologies under the Net-Zero Industry Act (Regulation (EU) 2024/1735 of 13 June 2024).

[85] IEA, Energy and AI, International Energy Agency, 2025.

[86] Ibid.

[87] IEA, Table A.4: Data Centres Electricity Consumption by Region, p. 110, Key Questions on Energy and AI, International Energy Agency, April 2026.

Material circularity remains another strategic challenge. The EU currently recovers less than 1% of rare earth elements from end-of-life products, while supply chains remain highly concentrated. In 2024, 95% of EU imports of rare earth elements came from China, Malaysia and Russia combined[88].

These developments underline the need for a system-level resource management approach, ensuring that the deployment of digital infrastructure remains compatible with energy system constraints, water availability and material sustainability, particularly in regions facing resource stress[89].

3.3.3. EU actions to unlock the twin green digital transition

The EU is deploying a broad policy toolbox that addresses both digitalisation as an enabler of sustainability and the sustainability of digital infrastructures themselves.

For instance, measuring and reducing the environmental footprint of telecommunications networks requires dedicated policy instruments. To this end, the Commission published in January 2026 an EU Code of Conduct (EU CoC) for the sustainability of telecommunications networks[90], as announced in the 2022 Digitalising the Energy System Action Plan[91]. The Commission consulted telecoms stakeholders broadly for the preparation of this EU CoC, which is voluntary. References to the EU CoC are included in the Commission's Digital Networks Act (DNA) proposal[92], which is currently in inter-institutional negotiations. Feedback from stakeholders that implement the EU CoC will generate data on sustainability in telecommunications networks, as part of the broader ICT sector. Telecoms stakeholders are therefore encouraged to implement the EU CoC and share their feedback.

In March 2026, the Commission proposed the Industrial Accelerator Act, providing a new set of measures to increase the demand for low-carbon and European-made technologies and products. Building on the Single Market, the proposal will boost sustainable manufacturing and accelerate industry's shift to cleaner, future-ready technologies.

In December 2025 the Commission also presented the European Strategy for Housing Construction, as part of the European Affordable Housing Plan. The Strategy aims to strengthen the productivity and innovation in construction and promoting advanced construction materials and methods, such as digitalisation, to increase resource efficiency.

[88] Euronews, Is Europe Losing the Race to Secure Rare Earth Materials?, January 2026; Eurostat, Imports of rare earth elements saw 30% drop in 2024, April 2025.

[89] IEA, Energy and AI, International Energy Agency, April 2025; IEA, Overcoming energy constraints is key to delivering on Europe's data centre goals, November 2025.

[90] European Commission, Environmentally sustainable telecommunications networks, January 2026.

[91] European Commission, Digitalising the Energy System – EU Action Plan, COM(2022) 552 final, 18 October 2022.

[92] European Commission, Proposal for a Regulation of the European Parliament and of the Council on Digital Networks (Digital Networks Act), COM(2026) 16 final, 21 January 2026.

The European Green Digital Coalition (EGDC) is an initiative of companies, supported by the European Commission and the European Parliament, which works towards supporting the green transition through digital technologies while reducing the environmental footprint of the ICT sector itself. In its first phase, launched in 2021, the EGDC developed a methodology for assessing the net climate impact of digital solutions. This helps policymakers and industry understand how digital technologies contribute to emissions reductions and supports access to green finance.

The second phase of the initiative began in March 2025 and focuses on applying this methodology to real world projects. Around fifty use cases across sectors such as energy, transport, agriculture and buildings are currently being analysed to demonstrate how digital solutions can reduce emissions while strengthening Europe's industrial competitiveness.

In addition, the Green Deal Data Space (GDDS), backed by the Digital Europe Programme, is bringing together over 500 datasets as well as implementing 10 use-cases[93] across the domains of climate, biodiversity, pollution, and the circular economy, assisting stakeholders in their pursuit of Green Deal objectives.

The Digital Product Passport (DPP) is a key instrument under the Ecodesign for Sustainable Products Regulation and an important element of the EU's circular economy framework. It introduces digital tools that allow information about products, such as materials used, repairability, recyclability and environmental performance, to be stored and accessed throughout the value chains. The DPP improves transparency and traceability of materials, facilitates recycling and secondary markets, and enables companies to demonstrate the sustainability performance of their products. It creates opportunities for European digital companies to develop new data infrastructures and services supporting circular value chains.

The Cloud and AI Development Act will address the urgent and growing data centre capacity gap, aiming to at least triple the EU's data centre capacity within the next five to seven years. It harmonises the conditions for investment in data centres across the EU, with a focus on sustainable and innovative data centres, ensuring their operators have access to land, finance and energy in the EU. Without strategic energy planning and a focus on sustainable infrastructures, data centre expansion will particularly challenge existing hubs and regions with high strain on natural resources, with a risk of crowding out electrification objectives in other sectors and generating increasing public opposition. Policy intervention is therefore essential to uphold consistency with the European Climate Law and ensure that possible national data centre acceleration policies do not result in a race-to-the-bottom in terms of sustainability and minimise environmental impacts and grid strain[94].

[93] Sage, the Data space for a sustainable Green Europe.

[94] The Shift Project, AI, data, and computing: shaping infrastructures for a decarbonised world, November 2025.

The Action Plan on Digitalising the Energy System continues to generate concrete policy outputs. Building on it, the Commission's Affordable Energy Action Plan of February 2025 announced a Strategic Roadmap for Digitalisation and AI in the Energy Sector, with a public consultation drawing over 300 contributions between August and November 2025[95]. The roadmap[96] will build on the 2022 Action Plan and set out measures to prepare for the energy system of tomorrow, including both challenges and opportunities linked to large-scale AI deployment in the energy sector. Specifically, it will establish an EU coordination framework to facilitate access to energy data and create a market for innovative services such as demand-side flexibility and bidirectional EV charging, build on ongoing work on smart grid indicators and digital twins for EU electricity networks, and improve the sustainable integration of data centres into EU electricity grids, including through a classification system and possibly minimum performance standards.

3.3.4. Member State actions towards the twin green and digital transition

Several Member States are also developing national approaches. Examples include digital product information tools supporting circularity, eco-design approaches for digital services, and national strategies on sustainable digitalisation and resource efficiency.

France has taken a legislative approach, combining the 2021 Climate and Resilience Law with an eco-responsible digital strategy and sector-specific measurement methodologies to reduce the environmental footprint of digital services, including requirements applicable to public digital services from 2024 and mandatory sustainable digital strategies for municipalities above 50 000 inhabitants from 2025[97]. The Netherlands is advancing the Sustainable Digitalisation Action Programme 2026-2028, with actions supporting companies to make more sustainable decisions, and monitoring the impact of the digital sector through an inventory of data. In Luxembourg, the Leneda platform, launched officially in March 2025 by transmission system operator Creos, provides consumers, producers and businesses with access to electricity and gas data, enabling monitoring of load profiles and consumption patterns, with energy market processes progressively integrated from spring 2025. Designed to eventually incorporate water and heat data, Leneda represents a concrete implementation of energy data space objectives at national level.

3.3.5. Reforms and investments needed to accelerate the green and digital transition

The Council conclusions on European Competitiveness in the Digital Decade of 5 December 2025 invite the Commission to develop targets related to a greener digital transition and to incentivise the

[95] European Commission, Digitalisation of the energy system.

[96] European Commission, Strategic Roadmap for digitalisation and AI in the energy sector – consultations opened, August 2025.

[97] République Française, Stratégie numérique responsable des collectivités : traduction opérationnelle du décret de l'article 35 de la loi REEN, July 2023.

deployment of sustainable and innovative technologies for climate action. Against this backdrop, several structural gaps need to be addressed.

Energy and water consumption data for the ICT sector remain fragmented and largely self-reported, although harmonised metrics for measuring the net climate impact of digital solutions are available at EU level as well as existing practices such as the Climate Neutral Data Centre Pact and the Energy Efficiency Directive. The environmental impact of digital infrastructures is measured through several existing frameworks, including the Energy Efficiency Directive delegated act for data centres, the WEEE Directive for e-waste, the EU CoC for sustainable telecoms networks, and the European Green Digital Coalition methodology for the net climate impact of digital solutions. However, implementation remains uneven across Member States, and coverage beyond data centres and telecoms KPIs is still partial.

Coordination between digital, energy and environmental authorities is uneven across Member States, and the alignment between EU research and innovation funding streams, Cohesion Policy and the European Competitiveness Fund remain insufficient.

Circularity of digital hardware is critically underdeveloped. Sovereign computing capacity, particularly for local AI inference within European jurisdictions, requires new models such as Hardware-as-a-Service. The speed of AI infrastructure deployment consistently outpaces permitting, reporting and grid integration systems, and the environmental externalities of compute-intensive AI systems are not yet internalised through financing mechanisms based on a polluter pays approach.

Recommendation:

Member States should advance the green digital transition by integrating sustainability into digital policies, investments and governance frameworks, by:

(i) strengthening coordination between national digital, energy and environmental authorities, integrating, where relevant, sustainability criteria into digital strategies policies and investments

(ii) supporting the development and uptake of harmonised environmental impact metrics for digital solutions and infrastructures, including energy consumptions and net carbon impact, building on established rules, methodologies and practices (Digital Coalition, Climate Neutral Data Centre Pact, Energy Efficiency Directive, EU Code of Conduct for the sustainability of telecommunications networks);

(iii) align EU research and innovation funding streams with Cohesion Policy and the European Competitiveness Fund to deploy environmentally beneficial digital solutions in transport, industrial processes, agriculture and climate action;

(iv) promoting circularity instruments and solutions such as the Digital Product Passport and Hardware-as-a-Service;

(v) ensuring national data centre expansion policies remain compatible with energy system constraints and environmental commitments and exploring incentive mechanisms for sustainable AI systems.

4. Funding the Digital Decade

Achieving the Digital Decade requires not only stronger policies and governance but also sustained and better targeted investment at both EU and national level. This section looks at how current funding instruments are supporting the digital transition, what implementation lessons can already be drawn from major programmes such as the Recovery and Resilience Facility (RRF), how cross-border investment mechanisms are evolving, and where the main financing gaps remain for the next programming period.

The digital transition is a core element of the Commission's investment strategy for competitiveness. The 2026 stocktaking exercise revealed that nearly all EU budget programmes contribute to the digital transition, channelling EUR 229 billion to that purpose between 2021 and 2025, representing almost 14.5% of the total EU budget for that period[98]. A significant share of the EU budget supporting the digital transition comes from the Recovery and Resilience Facility (RRF), which as of April 2026 accounts for EUR 133.1 billion in public digital investments.

Recovery and Resilience Facility (RRF) contribution to the Digital Decade targets

The recent Joint Research Centre (JRC) report shows that of this EUR 133 billion, EUR 120.4 billion is considered to be contributing directly to Digital Decade targets and objectives. Among the Digital Decade cardinal points, the largest estimated expenditure is dedicated to digitalisation of businesses (36%) and digitalisation of public services (31%), followed by digital skills (18%) and digital infrastructure (15%).

	RRF budget (EUR million)
Other DD objectives	12 733
Basic digital skills	13 110
ICT specialists	8 713
Gigabit network coverage	10 195
5G coverage	1 654
Semiconductors	4 917
Edge nodes	0
Quantum computing	985
Cloud computing services	5 453
Data analytics	4 665

[98] The 2026 stocktaking exercise to estimate EU spending on the digital transition was conducted for the implementation of the 2021-2027 EU budget over the 2021-2025 period: European Commission, Digital tracking.

Artificial Intelligence	5 219
SMEs digital intensity	13 994
Unicorns	13 997
e-ID	445
Digital public services	23 593
Electronic health records	13 455
Total DD-relevant budget	120 396

Source: JRC Calculations

In addition, a total of 25% of the RRF reforms are aimed at strengthening public institutions, the digitalisation of public services, education and cybersecurity, while 13% improve skills and labour market outcomes[99]. Over 55% of RRF funds have been disbursed[100], with significant implementation progress during the last reporting period[101], although the Commission stressed that implementation needs to accelerate in most Member States.

By 2030, digital RRF investments are estimated to generate a cumulative economic impact of EUR 219 billion within the EU and EUR 302 billion globally (corresponding to a multiplier of 1.5 within the EU and 2.0 globally, significantly higher than the overall impact of RRF spending)[102]. Of the total EU impact, around EUR 51 billion arises from cross-border spillover effects, confirming the Single Market as a key transmission channel and reinforcing the case for coordinated EU action.

Lessons learned from implementation of digital measures under the RRF, as shared in the Digital Decade Board, reflecting the views from Spain, Croatia, Hungary, Ireland, Italy, Lithuania, Luxembourg, Malta and Portugal, point to a common set of delivery constraints and design improvements for the future programming period. First, administrative burden and reporting requirements often proved disproportionate, particularly for smaller projects for which complex compliance obligations can undermine accessibility and effectiveness unless proportionality is built into control and audit expectations. Secondly, in large-scale initiatives, implementation delays were frequently driven by complex public procurement procedures, demanding data integration and interoperability requirements, and an underestimation of the digital maturity of existing (often legacy) systems. Progress also became highly dependent on suppliers, meaning that even minor setbacks could stall entire programmes. Thirdly, digital policy and especially innovative and advanced technologies require greater design flexibility: projects involving fast-evolving solutions need space for testing, pilots and iterative development, alongside more adaptable milestones, targets and implementation pathways. These challenges are compounded by limited specialised expertise within Member States and by the inherent difficulty of

[99] European Commission, Recovery and Resilience Facility Annual Report 2025 - Reforms and Investments, October 2025.

[100] As of August 31, 2025.

[101] Referred to the period between 1 September 2024 and 31 August 2025.

[102] Michels, A., Ferreira, V., Annoni, P., Burton, J., Pedauga, L., Rueda-Cantuche, J. M. & Kušen, M., European Economy. Discussion Paper 249: Digital Measures under the Recovery and Resilience Facility: Economic Impacts at Macro, Sectoral and Country Levels, European Commission, Directorate-General for Economic and Financial Affairs, 2026.

forecasting demand and uptake for novel digital technologies. Finally, implementation would benefit from stronger multi-level coordination that better reflects the operational role of regional and local authorities, with clearer allocation of responsibilities and decision-making across EU, national and regional levels to reduce friction, improve sequencing and accelerate delivery.

Advancing cross-border collaboration for digital investments

Through multi-country projects (MCPs), Member States and the Commission are stepping up cooperation to build strategic digital capacities that no single country could deliver alone. In 2025-2026, this has led to tangible progress in setting up and advancing European Digital Infrastructure Consortia (EDICs).

Two new EDICs have been established: the Digital Commons EDIC, which aims to support the development and scaling of digital commons by improving access to funding and strengthening public contributions; and the IMPACTS-EDIC, which focuses on enhancing public services through innovative interoperability solutions.

In parallel, **earlier initiatives have moved from planning to implementation**. The Alliance for Language Technologies (ALT-EDIC) has begun deploying newest Language Technologies in domains such as public services, telecommunications, energy and science. The Local Digital Twins towards the CitiVERSE EDIC (LDT EDIC) became fully operational following the appointment of its director in November 2025. In addition, the EUROPEUM-EDIC completed the transfer of the European Blockchain Services Infrastructure from the European Commission in the first quarter of 2026.

Moreover, formal applications for new EDICs have been submitted to the Commission in areas such as cybersecurity skills and agri-food, with additional proposals - particularly in genomics and mobility - expected in 2026 or early 2027. These developments open important opportunities to scale interoperable infrastructures, pool investments and strengthen Europe's digital sovereignty, but they also highlight challenges related to governance complexity, long-term sustainability and effective uptake.

Overall, these developments show a shift from coordination to concrete delivery, with EDICs increasingly operational, expanding their membership and starting to produce initial results. An updated overview of the EDICs established is available at the Commission webpage of the European Digital Infrastructure Consortia.

Member States are also advancing **Important Projects of Common European Interest (IPCEIs).** Existing initiatives in microelectronics (IPCEI-ME/CT) and cloud (IPCEI-CIS) are now fully operational and mobilising substantial public and private investments. The recently approved Tech4Cure IPCEI is expected to drive innovation in AI-enabled healthcare. Meanwhile, new IPCEI candidates are under design in strategic areas such as AI technologies, computing infrastructure and advanced semiconductor technologies.

Investment needs for the digital transition

Public funding also needs to ensure the right balance between budget predictability and flexibility. While a stable and predictable trajectory needs to be the basis for budget planning, the fast-evolving nature of technological development requires the ability to respond swiftly to emerging priorities and trends in certain areas. Joint Undertakings (JUs), for instance, are well equipped in this regard, with agile procedures that allow them to adapt work programmes swiftly when new urgencies arise. By pooling public and private resources at scale, JUs have played a pivotal role in aligning strategic agendas, and fostering robust ecosystems around key EU policy priorities, thereby strengthening Europe's competitiveness and technological sovereignty. However, Member States' financial planning has not always been sufficiently flexible to accommodate emerging needs and changing priorities, at the pace required by the fast pace of technological development. **Beyond 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 2026, InvestEU has mobilised finance for investments for EUR 318 billion, out of which more than EUR 200 billion from private sources. Out of those, EUR 23.34 billion is supporting digitisation and EUR 13.44 billion are related to strategic investments on critical infrastructure, cybersecurity, space and defence.

However, financial instruments are not yet fully taken advantage of in all programmes[103] and often lack a strong policy steer or the scale needed to address systemic investment gaps. Blending instruments and budgetary 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[104]. Overall, the EU faces a substantial and urgent need to increase investment in digital technologies, infrastructure, and innovation ecosystems, particularly in equity. A savings and investments union with a fully integrated capital market is fundamental to providing European businesses with the equity capital they need to innovate and grow. 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. This is of particular importance, considering also the fact that it is expected that 58% of the public budget of digital measures in Digital Decade National Roadmaps will phase out by the end of 2027. **This poses a near-term risk of a significant investment shortfall**, with a potential one to two years gap notably between the expiry of RRF-funded measures and the operational deployment of the European Competitiveness Fund and NRPPs under the next Multiannual Financial Framework.

[103] 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: European Commission, Digital Tracking.

[104] European Commission, Interim Evaluation of the InvestEU Programme – Final Report, 1 October 2024.

Europe must urgently tackle its structural shortage of private risk capital, and in particular equity, for high-growth and deep-tech companies as well as large infrastructural investments. There is indeed the need for an urgent reflection on the means to boost European equity capacities at scale to finance Europe's tech sovereignty ambitions.

To **bridge the gap between research and market**, more actions and investments are required, particularly at Technology Readiness Level (TRL) 6, to support the prototyping and commercialisation of digital technologies. Additionally, there is a need for public and private **investment in fostering the growth-stage of companies**, as evidenced by a significant drop in the number of scaleups compared to startups in the EU.

Establishing and scaling **regulatory and technical sandboxes is also a priority**, as they enable companies, especially SMEs and startups, to test innovative technologies in controlled, real-world environments under regulatory supervision. Another essential area of investment is in **enabling infrastructure, such as secure and scalable cloud and edge computing services, as well as interoperable data infrastructures**, which underpin a wide range of advanced digital technologies, such as AI.

Digital transformation requires substantial upfront spending on infrastructure, software, and skills. Firms' investments are constrained by uncertain or long-term returns on investment, combined with limited access to finance. In its Multiannual Financial Framework proposal, which set out the approach for the EU budget between 2028 and 2034, the Commission has proposed EUR 234.3 billion for a new European Competitiveness Fund (ECF). Part of it will support the digital transition, invest in strategic technologies and simplify EU funding. The Commission proposal for the ECF refers to the Digital Decade Policy Programme 2030: "In particular, the ECF's digital investments respond to the gaps and priorities identified in the State of the Digital Decade 2025 report, notably in digital connectivity, advanced computing, and digital skills, supporting the Union's objective of digital sovereignty".

The Commission proposal for the next Multiannual Financial Framework includes a significantly increased budget for digital. The proposed budgetary envelope is EUR 68.3 billion, combining **EUR 51.5 billion funding from the ECF**[105] and **EUR 16.8 billion from the next Research and Innovation Framework Programme (FP10)**[106] under a shared Digital Leadership window. The digital window brings together major digital programmes such as the current Digital Europe Programme (DIGITAL), the Connecting Europe Facility's (CEF) Digital strand and the collaborative and applied research part of Horizon Europe's Pillar II. **Horizon Europe will remain a standalone programme but with a structure that is closely aligned**

[105] EurLex, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing the European Competitiveness Fund ('ECF'), including the specific programme for defence research and innovation activities, repealing Regulations (EU) 2021/522, (EU) 2021/694, (EU) 2021/697, (EU) 2021/783, repealing provisions of Regulations (EU) 2021/696, (EU) 2023/588, and amending Regulation (EU), July 2025.

[106] EurLex, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing Horizon Europe, the Framework Programme for Research and Innovation, for the period 2028-2034 laying down its rules for participation and dissemination, and repealing Regulation (EU) 2021/695, July 2025.

with the ECF, under a single policy steer, thus coherently covering all aspects of digital, from research to advanced digital skills, digital infrastructures, critical digital technologies, their ecosystems and applications.

The proposal also aims to leverage substantially more private and public investment, including through equity and blended for start-up and scaling. **The ECF InvestEU instrument will leverage public and private funding** towards EU priority sectors, with a minimum EU support of EUR 17 billion which can be further topped up from the ECF policy windows.

Given the number of different funding streams supporting digital objectives, it will be important to ensure proper triangulation between them. The use of large-scale project implementation mechanisms with potential to pool resources from different funding streams, such as EDICs, would benefit from closer cooperation between the Commission and the Member States.

Recommendation:

The EU and Member States should strengthen further their cooperation, acting not only as a de-risking partner but also as a strategic market aggregator, mobilising demand and investment at European scale to support the breakthrough technologies required to strengthen technological sovereignty and close Europe's innovation gap.

Member States should align the implementation of the Digital Decade with the future architecture of the next Multiannual Financial Framework, by:

(i) clearly outlining in their updated National Roadmaps how they intend to use their NRPP allocations, ensuring full alignment with DDPP priorities and the ECF's digital objectives, and minimising the risk of disruption to investment flows, while maintaining coherence, transparency and strategic targeting of investments;

(ii) assessing and reporting on expected and actual progress on these planned measures, using their own specified measures and, where appropriate, complementary data sources, to provide a robust and evidence-based estimation of implementation outcomes;

(iii) appointing National Contact Points for EDICs at national level, to capitalise on existing know-how and best practices and to streamline the process of setting up European Digital Infrastructure Consortia.

5. International

International cooperation on digital policy focuses on boosting European competitiveness, promoting the security of Europe and its partners, and shaping global digital governance and standards. To that end, the European Commission and the High Representative for Foreign Affairs and Security Policy adopted an International Digital Strategy for the European Union in June 2025, with the following objectives: (i) to expand international partnerships, for strengthening EU tech competitiveness and security as well as that

of its partners (ii) to deploy an EU Tech Business Offer, by combining EU private and public sector investments to support the digital transition of partner countries (iii) to strengthen global digital governance, by promoting a rules-based global digital order, in line with the EU's fundamental values

The Commission has continued to develop and deepen its network of Trade and Technology Councils (TTC) and Digital Partnerships with partners, including India, Japan, the Republic of Korea, Singapore and Canada, developing cooperation on research and innovation collaboration, industry cooperation, regulatory and policy exchanges as well as standardisation. To that end, in 2025, the Commission held Digital Partnership Councils with Japan, the Republic of Korea, Singapore and Canada.

In the Latin America and Caribbean (LAC) region, bilateral digital dialogues have been established with Brazil, Argentina and Mexico, complemented by bi-regional activities under the EU-LAC Digital Alliance. The EU-LAC Digital Alliance Week was held in September 2025, in Guatemala. It aimed at stocktaking of its achievements and paved the way to the IV EU-CELAC Summit in Colombia, in November 2025.

The Global Gateway initiative focuses on digital infrastructure investments to help bridge the global digital divide and enhance secure digital connections, supporting the EU's digital resilience and reducing dependencies. Under the Global Gateway, the Digital for Development (D4D) Hub has provided a strategic platform to strengthen digital cooperation between the European Union and its Member States (Team Europe) and partners in Africa, Asia-Pacific, Latin America and the Caribbean, and the EU neighbouring countries. The Tech Business Offer implementation was initiated with high-level events focused on showcasing EU solutions to the Latin-American countries at the EU-LAC Digital Alliance, and country-specific events in 2025 with Nigeria and Viet Nam. Next to this, several outreach events for companies in EU Member States were held in 2025.

The Commission continued to support digital transformation efforts in enlargement countries and the EU neighbourhood. Preparatory work was completed for Ukraine and Moldova to join the EU's Roam Like At Home area on 1st January 2026. The Commission supported the integrity of the presidential and parliamentary elections in Moldova. The Reform Agendas of the Western Balkan countries adopted in October 2024 provide timelines for legislative alignment with EU digital acquis from December 2024 to December 2027.

The Commission has also engaged in multilateral fora, notably marking progress on the governance of artificial intelligence (G7 Hiroshima AI Process, Council of Europe Convention, OECD). To improve its economic resilience and protect sensitive technologies, the EU has implemented measures such as the EU Economic Security Strategy, promoting cooperation with key partners in emerging technologies. These measures aim to balance economic openness with strategic interests and to enhance the EU's resilience in critical sectors.

Trade policy and agreements also play a vital role in this regard, by setting the global and bilateral rules for digital trade in an open but assertive manner, based on European values. The Commission negotiated

ambitious commitments on digital trade with Singapore and the Republic of Korea and in recent trade agreements with New Zealand, India, Chile and Japan.

The EU also sees increasing opportunities for cooperation with Gulf Cooperation Council (GCC) countries in AI, submarine cables, digital identity and e-signatures, and secure connectivity. In December 2025, the EU launched negotiations of Strategic Partnership Agreements (SPAs) with the Kingdom of Saudi Arabia, United Arab Emirates and Qatar.

The EU faces critical geopolitical challenges centred on security, economic sovereignty, and internal cohesion, driven by Russia's ongoing aggression in Ukraine, instability in the Middle East, and intense rivalry between the US and China. Key imperatives include fostering strategic autonomy, managing industrial dependencies on China, navigating potential US security shifts, and accelerating enlargement to secure the neighbourhood.

Recommendation:

Member States should:

(i) be involved in developing and implementing the EU's Digital Partnerships, Dialogues and Trade and Technology Councils and their priorities, in full respect of the EU's institutional framework. The close involvement of EU tech businesses and other relevant stakeholders, including civil society and the research community, will be indispensable for the collective advancement of shared goals.

(ii) actively promote the EU Tech Business Offer to ensure that European companies, including SMEs, start-ups, scale-ups and large companies, are informed and involved in the structuring of the Offer and can fully benefit from this initiative.

(iii) regularly update on their contribution to the implementation of the EU's International Digital Strategy, in particular their international activities complementing it.