EUROPEAN
COMMISSION

Brussels, 16.6.2025
SWD(2025) 290 final

COMMISSION STAFF WORKING DOCUMENT

Digital Decade in 2025: progress and outlook

Accompanying the document

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

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

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

European Commission

DIGITAL DECADE IN 2025: PROGRESS AND OUTLOOK

1 Technological sovereignty, security and competitiveness 2
1.1 A continent supporting digital innovation and sovereignty 2
1.2 Digitally transformed and competitive industries 38
1.3 A secure continent 54
2 Protect and empower people, preserve EU democracy and values 66
2.1 Empower people through digital skills 66
2.2 Deploy digital solutions for people and societies 81
2.3 Protect people, including minors, online 91
2.4 Protect information integrity and democracy 97
3 Harnessing digitalisation for the green transition 102
3.1 Key trends and prospects 103
3.2 Addressing the environmental footprint of digitalisation 107
3.3 Development of concrete digital policies and tools for the green transition 113
3.4 Green/digital twin transition measures at Member State level 116
4 Coherence and synergy: aligning digital policies and funding at different levels 121
4.1 Better and lighter digital legislation 121
4.2 EU funding for the Digital Decade: state of play 125
4.3 Cooperation with cities and regions as a tool for implementing and disseminating digital policy 135
4.4 The international dimension of the Digital Decade 139

1 Technological sovereignty, security and competitiveness

The digital transformation is at the heart of the EU's strategy to enhance competitiveness, to drive economic growth while ensuring economic security, and to safeguard its sovereignty. The Political Guidelines 2024-2029[1] task the new Commission to drive the EU's progress towards a more competitive resilient and inclusive future, which implies **attaining leadership in strategic technologies, establishing essential assets for technological sovereignty and resilience, and fostering the commercialisation of deep tech innovation.**

The mandate of the Executive Vice President for *Technological Sovereignty, Security and Democracy*[2] emphasises the need to increase investments in frontier technologies where the EU can: have a competitive edge over its competitors; enhance existing digital capabilities; develop and deploy resilient, secure infrastructures; improve access to secure, fast and reliable connectivity; strengthen economic security; foster the uptake of digital technologies by public administrations and businesses; and create strong, innovative, interoperable digital ecosystems and digital public infrastructures across the EU.

The central role of digitalisation and digital technologies has been also highlighted in the reports on **'The future of EU competitiveness'**[3] and on **'The Future of the Single Market'**[4]. The Letta report calls for a harmonised digital single market enabling seamless digital services across borders, and emphasises the need to support European tech champions and create a business environment that is conducive to scaling start-ups across the EU. The Draghi report emphasises the urgency of bold action to close the innovation gap, compete in the global tech race and identify critical gaps in achieving the EU's targets, such as digital skills, connectivity, secure and sovereign cloud infrastructure, and capabilities in strategic sectors such as semiconductors and quantum technologies. It also underscores the importance of not only boosting the EU's competitiveness but also enhancing its sovereignty and resilience and addressing the EU's reliance on non-EU providers in critical technology areas.

Digital technologies also play a crucial role in advancing the EU's economic security, underpinning its ability to defend its economic interests, lead in innovation, protect its citizens and shape the rules of the global economy.

1.1 A continent supporting digital innovation and sovereignty

In an era of rapid technological change and intensifying global competition, the EU faces critical challenges in maintaining its digital leadership and ensuring its economic security. Persistent barriers, including a fragmented Single Market, continue to hinder the EU's ability to innovate and scale up

---

[1] European Commission, Europe's Choice, Political Guidelines for the next European Commission 2024–2029, 2024.
[2] European Commission, Mission Letter to Henna Virkkunen, 2024.
[3] Draghi, M., The Future of European Competitiveness, 2024 (hereafter referred to as the "Draghi Report").
[4] Letta, E., Much More Than a Market: Report by Enrico Letta on the Future of the Single Market, 2024 (hereafter referred to as the "Letta Report").

digital solutions effectively. Divergent national regulations, insufficient interoperability and still too limited cross-border cooperation constrain the growth of a truly integrated European digital ecosystem. This fragmentation not only stifles innovation and competitiveness, but also weakens the EU's capacity to develop homegrown tech champions.

At the same time, (economic) security risks related to strategic dependencies in global supply chains or rising geopolitical and geoeconomic tensions underscore the urgent need to improve our technological sovereignty.

Addressing these challenges requires strengthening the research and innovation (R&I) ecosystem, **fostering the growth of innovative businesses**, and **advancing strategic infrastructure**, including advanced connectivity, semiconductors, cloud and edge computing, quantum technologies, and high-performance computing (HPC).

The development of a **digital euro** will play a crucial role in ensuring Europe's economic autonomy, complementing existing payment systems while enhancing security, efficiency, and accessibility. In addition, the **EU Digital Identity Wallets** form a core component of Europe's digital public infrastructure, providing trusted, standardised tools for secure digital interactions. This infrastructure will be complemented by the introduction of **European Business Wallets**, which will serve as strategic enablers for a more competitive and innovation-driven digital economy by reducing administrative burdens, enhancing regulatory certainty, and unlocking new opportunities for digital service delivery and cross-border market participation.

The following sections outline these priorities, providing an overview of the current state and key policy developments.

1.1.1 R&I for technological leadership and economic security

R&I supporting technological leadership

The EU has important strengths in the field of research and innovation. However, its weaknesses are becoming more and more apparent.

Among the most important challenges is the limited scale of **investment in research and innovation**, with only 10% occurring at the EU level and the lack of focus on breakthrough innovation[5].

In 2023, expenditure on R&D in the EU reached EUR 381 billion, or 2.22% of EU GDP, below the 3% target[6]. The **private sector also lags behind**, with EU companies investing approximately EUR 270 billion less in R&D than their US counterparts in 2021[7].

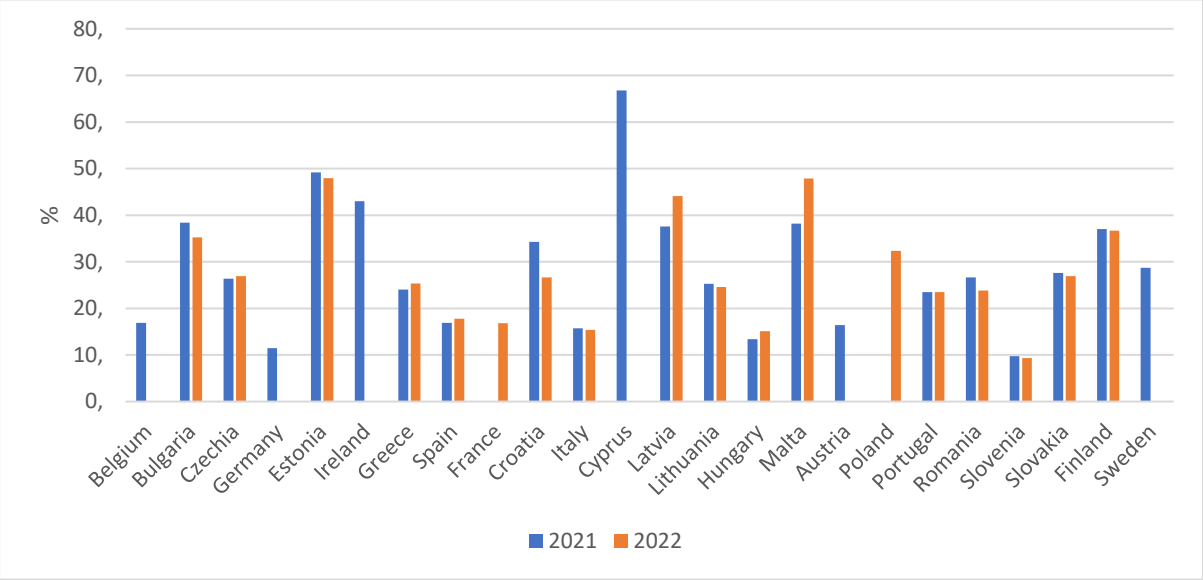
Lower levels of R&D&I investment generally translate into lower shares of gross value added (GVA). The ICT sector is generally a major performer in terms of R&D. The relation between R&I spending and GVA is usually mutually reinforcing. This means that countries that invest more in R&I, will tend to have higher productivity and value creation. The opposite is also true.

[5] Draghi, M., The future of European competitiveness, 2024. Part A – A competitiveness strategy for Europe.
[6] Eurostat, R&D expenditure, 2024.
[7] Draghi, M., The future of European competitiveness, 2024. Part A – A competitiveness strategy for Europe.

In the EU, the trends are not encouraging. According to Eurostat data, the percentage of the ICT sector in GVA is relatively low and grew only marginally in recent years, from 4.86% in 2019 to 5.46% in 2022[8].

Moreover, Eurostat data on business expenditure on R&D[9] and on R&D personnel in ICT sector[10] shows a slightly decreasing trend between 2021 and 2022 in most of the Member States for which data is available across the two years.

Figure 1. Business expenditure on R&D (BERD) in ICT sector as % of total R&D expenditure, 2021 and 2022 (missing for both years for DK, LU, NL)



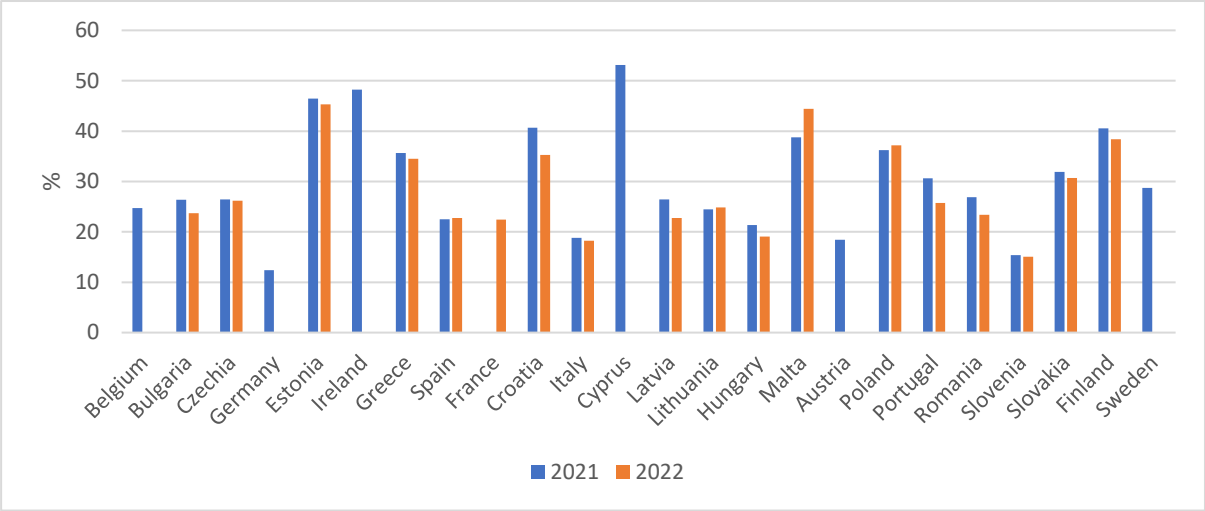
Source: Eurostat

[8] Eurostat, 2025. This indicator measures the importance of the ICT sector in the economy. A strong ICT sector often indicates strong innovation ecosystems. A high share of value added may suggest a significant role in global ICT markets, reducing reliance on external providers.

[9] Eurostat, Business Expenditure on R&D (BERD) in ICT Sector as % of total R&D Expenditure by NACE Rev. 2 Activity, 2025. This indicator shows a decrease for 9 Member States, out of the 16 Member States for which data is available.

[10] Eurostat, R&D Personnel in ICT Sector as % of Total R&D Personnel by NACE Rev. 2 Activity, 2025. This indicator shows a decrease for 13 Member States, out of the 17 Member States for which data is available.

Figure 2: R&D personnel in ICT sector as % of total R&D personnel, 2021 and 2022 (missing for both years for DK, LU and NL)



Source: Eurostat

The EU is still weak on **transforming scientific knowledge into patents**. A study of 221 emerging technologies across 12 clusters highlights **Europe's role in scientific knowledge production**. While the US and China lead, Europe maintains strong research positions in Digital Twin, AI & Machine Learning, Therapeutics & Biotechnologies, Energy, and Environment & Agriculture.

European organisations contribute significantly to high-impact scientific publications but lag in patenting, filing fewer applications than the US and China. Europe serves as a global hub for scientific exchange but lacks critical mass among top-performing entities, reflecting a fragmented ecosystem with limited specialisation beyond AI & Machine Learning[11]. While the volume and impact of EU research is comparable to the output of the two leading economies (China and US), the fact that EU organisations are not in the top rankings suggests that research is scattered across multiple organisations rather than centralised. This means weaker international visibility and difficulties in attracting top-tier international talent to EU universities and research centres. It may also translate into duplication of research efforts, diluted funding, and limited pooling of resources such as infrastructure, data or human capital.

Figure 3: Translation ratio (patents/scientific publications) for each category for EU, US, China, Japan and South Korea

	EU	US	China	UK	Japan	South Korea	India	Row
Advanced Materials and advanced manufacturing	0.96%	6.31%	10.30%	0.58%	4.31%	5.29%	0.41%	0.84%
Air and Space	4.94%	3.23%	8.46%	1.43%	28.24%	18.55%	0.00%	1.02%
Mobility and Transport	0.81%	2.54%	10.05%	0.71%	1.75%	9.18%	1.61%	1.20%
Digital twin	1.08%	12.62%	41.34%	0.00%	3.33%	22.33%	3.16%	1.36%
Artificial intelligence and Machine learning	0.51%	2.43%	17.42%	0.78%	0.32%	8.00%	0.63%	0.43%
ICT	1.11%	17.30%	2.85%	0.95%	18.84%	94.33%	0.37%	1.36%
Medical imaging	0.00%	0.60%	0.37%	0.00%	0.00%	0.00%	0.00%	0.00%
Therapeutics and Biotechnologies	1.11%	3.96%	17.36%	1.20%	0.49%	15.18%	0.95%	1.36%
e-Health	0.78%	2.65%	19.61%	0.00%	2.73%	10.22%	0.28%	0.69%
Environment and Agriculture	1.14%	4.44%	5.83%	0.80%	3.24%	29.03%	0.51%	1.64%
Energy	0.77%	4.27%	16.00%	3.08%	0.85%	6.55%	0.67%	1.11%
Quantum and Cryptography	1.54%	7.32%	19.45%	2.74%	1.90%	9.42%	0.73%	1.76%

Source: JRC

These results are corroborated by the **EU Industrial R&D Investment Scoreboard**[12], which monitors and benchmarks the performance of the EU's leading industrial R&D investors against their global peers. In the Scoreboard, the **digital sector**[13] has experienced the highest growth in R&D investment over the past 20 years and is characterised by high R&D intensity. However, EU digital companies have struggled to scale up and compete effectively on a global level.

US companies dominate digital R&D, with 40% of digital companies and 53% of total investment for Scoreboard companies in 2023. Alphabet and Meta alone accounted for 12.6% of global digital R&D (EUR 72 billion), surpassing the combined total of EU-based digital firms (8.9%). **China has significantly increased its digital R&D share** from 7.1% in 2014 to 19.4% in 2023, with Huawei tripling its expenditure to EUR 18.8 billion.

---

[11] Joint Research Centre (Eulaerts, O., Grabowska, M. and Bergamini, M.) *Weak signals in Science and Technologies - 2024*, Publications Office of the European Union, Luxembourg, 2025, JRC140959. The report uses data on scientific publications and patents, covering the time period 1996- 2023.

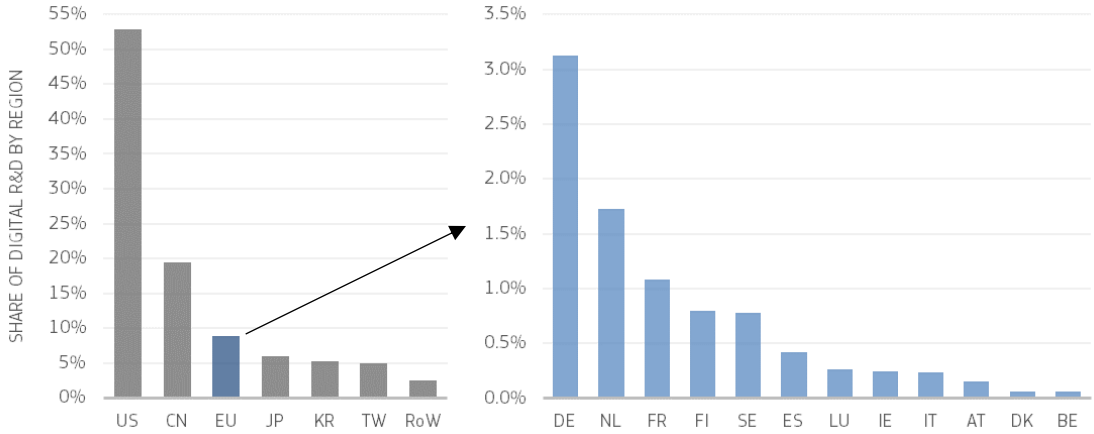
[12] Joint Research Centre (Nindl, E., Napolitano, L., Confraria, H., Rentocchini, F., Fako, P., Gavinan, J. and Tuebke, A., The 2024 EU Industrial R&D Investment Scoreboard.) *The 2024 EU Industrial R&D Investment Scoreboard*, Publications Office of the European Union, Luxembourg, 2024.

[13] The study defines the digital sector as comprising firms within the information and communication technologies (ICT) software and hardware sectors, as identified in the EU Industrial R&D Investment Scoreboard. These two sectors encompass ICB 4-digit categories, including ICT Software (covering computer services, software, and telecommunication services) and ICT Hardware (encompassing computer hardware, semiconductors, and telecommunications/electronic equipment).

Meanwhile, **the EU's global share declined** from 13.7% to 8.9%. Of the 58 EU digital companies in the 2024 Scoreboard, most are based in Germany (17), the Netherlands (10), and France (9), while 16 EU countries have no top digital R&D firms. Only five EU companies–SAP, Siemens, Nokia, Ericsson, and ASML–rank among the top 30 digital R&D investors, with SAP (15th) as the only EU software firm in the top 50.

Between 2019 and 2023, the largest R&D investment increases in the EU came from ASML (+ EUR 1.19 billion), SAP (+ EUR 980 million), and Infineon Technologies (+ EUR 738 million). Companies that tripled R&D investment over this period include ASML, Spotify, ASM International, Elastic, and Sartorius, signalling momentum in semiconductor technologies.

Figure 4: R&D investment shares by global region and EU country in digital sectors. 2023



Source: The 2024 EU Industrial R&D Investment Scoreboard, European Commission, JRC/DG R&I

Dependencies and economic security

The EU's ambition to achieve technological leadership in some areas, and retain it in others is complicated by an unstable geopolitical climate due to issues such as intensifying strategic competition between the US and China and the fallout from the Russian invasion of Ukraine. Russia's war of aggression against Ukraine has sparked inflation and energy price increases, and has led to a review of the EU's budget thus moving funds from certain priorities to others[14]. At the same time, it has further highlighted the bloc's critical dependencies on external suppliers, already made evident from the COVID-19 pandemic.

Disruptive new technologies, together with strategic competition over critical raw materials, are linking economic and security interests more closely together[15]. This has brought the EU to examine its technological competitiveness lag and critical dependencies, which could translate into serious risks to the EU's economy and security in terms of their potential for weaponisation.

Today, the EU is still lacking a significant domestic semiconductor manufacturing capacity, and no capacity to manufacture the leading-edge chips that are vital for all electronic devices, digital services

[14] European Commission, *EU budget today*. Available at: https://commission.europa.eu/strategy-and-policy/eu-budget/motion/today_en

[15] European Commission, Report: Safer *Together – Strengthening Europe's Civilian and Military Preparedness and Readiness*, 2004.

and technologies in AI, defence, and other advanced applications[16]. Around 70% of foundational AI models have been developed in the US since 2017. Additionally, the largest EU cloud operator has a mere 2% share of the EU market, and none of the top ten global tech companies in terms of quantum investment are based in the EU.

In the semiconductor value chain, EU companies have strengths in equipment for chip manufacturing; however, they are weaker in the intermediate inputs and chip-production segments, relying heavily on imports: 80% of EU companies' suppliers are headquartered outside the EU, with 35% located in the US, 12.4% in Taiwan, 11.7% in China or Hong Kong, 10% in South Korea, and nearly 9% in Japan; in addition, European companies have a significant share of their customers in semiconductors (63%) headquartered outside the EU[17].

Initiatives under the **Economic Security Strategy**[18] aim to address these risks by promoting the EU's competitiveness, protecting it against economic security risks, and partnering with like-minded non-EU countries that share mutual interests to address common concerns. Digital technologies are central to the Strategy and to the Commission Recommendation on critical technology areas for the economic security of the EU[19]. Together with the Member States, the Commission has initiated a number of **risk assessments covering semiconductors, quantum technologies, AI and biotech,** which will support decision-making on targeted and proportionate mitigation strategies.

To protect against technology leakage, the EU adopted an **Economic Security package** in January 2024[20], which was followed up by several initiatives in 2024 and 2025.

In May 2024, the Council adopted a Recommendation on **enhancing research security**[21], in response to the growing geopolitical risks and the evolving landscape of international research and innovation. Special emphasis is placed on **high-risk research areas, such as artificial intelligence, quantum computing, biotechnology, and advanced materials**, which have the potential for dual-use applications. Member States are encouraged to closely monitor these areas and implement stricter security measures as necessary. Moreover, the Council Recommendation points to enhancing cybersecurity practices, ensuring better protection for sensitive research data, and increasing awareness among researchers and institutions about the potential security risks.

In January 2025, the Commission published a **Recommendation on reviewing outbound investments in technology areas critical for the economic security of the Union**[22]. Outbound investment screening could serve as a complementary tool to export controls on dual-use goods and could prevent the export of sensitive technologies or know-how of EU companies through investments in non-EU countries where the boundaries between civil and military activities, for example, are

---

[16] IC Insights, McClean Report, 2022.

[17] Ciani, A., Nardo, M., The position of the EU in the semiconductor value chain: evidence on trade, foreign acquisitions, and ownership, European Commission, Ispra, 2022, JRC129035.

[18] Joint communication to the European Parliament, the European Council and the Council on 'European economic security strategy', 2023 JOIN/2023/20 final.

[19] Commission Recommendation (EU) 2023/2113 of 3 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States (C/2023/6689), OJ L 202, 4.10.2023

[20] European Commission, New tools to reinforce the EU's economic security, 2024.

[21] Council recommendation on enhancing research security, C/2024/3510, 2024.

[22] Commission Recommendation (EU) 2025/63 of 15 January 2025 on reviewing outbound investments in technology areas critical for the economic security of the Union (https://eur-lex.europa.eu/eli/reco/2025/63/oj/eng)

blurred. The Commission Recommendation covers three technology areas: advanced semiconductors, artificial intelligence and quantum technologies.

The EU also protects its most sensitive technologies and critical infrastructure, particularly those of common European interest, against malign foreign acquisitions through its **FDI Screening Regulation**[23], which is has been **under revision** in 2024. The Commission has proposed to ensure that all Member States have a screening mechanism in place with a minimum sectoral scope that applies to investment also by European companies that are ultimately controlled by individuals or businesses from a non-EU country.

The EU has been setting up Digital Partnerships with countries like Canada, Japan, South Korea and Singapore to advance joint frontier technologies research collaboration in the fields of, for instance, semiconductors, high-performance and quantum technologies, and 5G/6G. Furthermore, the EU has also concluded several critical channels of communications with India, Japan, Singapore, and the US to give early warning of disruptions of the semiconductors supply chain, thus enhancing supply chain resilience.

1.1.2 Innovative start-ups and scale-ups in the EU

The EU's economic competitiveness critically depends on the ability of innovative start-ups and scale-ups to access capital, notably those active in areas such as Artificial Intelligence (AI), quantum and other Deep Tech fields, biotech and cleantech.

Progress towards the Digital Decade target

Target: The digital transformation of businesses, where the Union facilitates the growth of its innovative scale-ups and improves their access to finance, leading to at least doubling the number of unicorns.

KPI definition: Unicorns are measured as the sum of unicorns referred to in Article 2, point (11)(a), of the Decision and those referred to in Article 2, point (11)(b), of that Decision.

Source: Dealroom platform[24].

Available data points: from 2008 to 2024.

2024 data value[25]: 286.

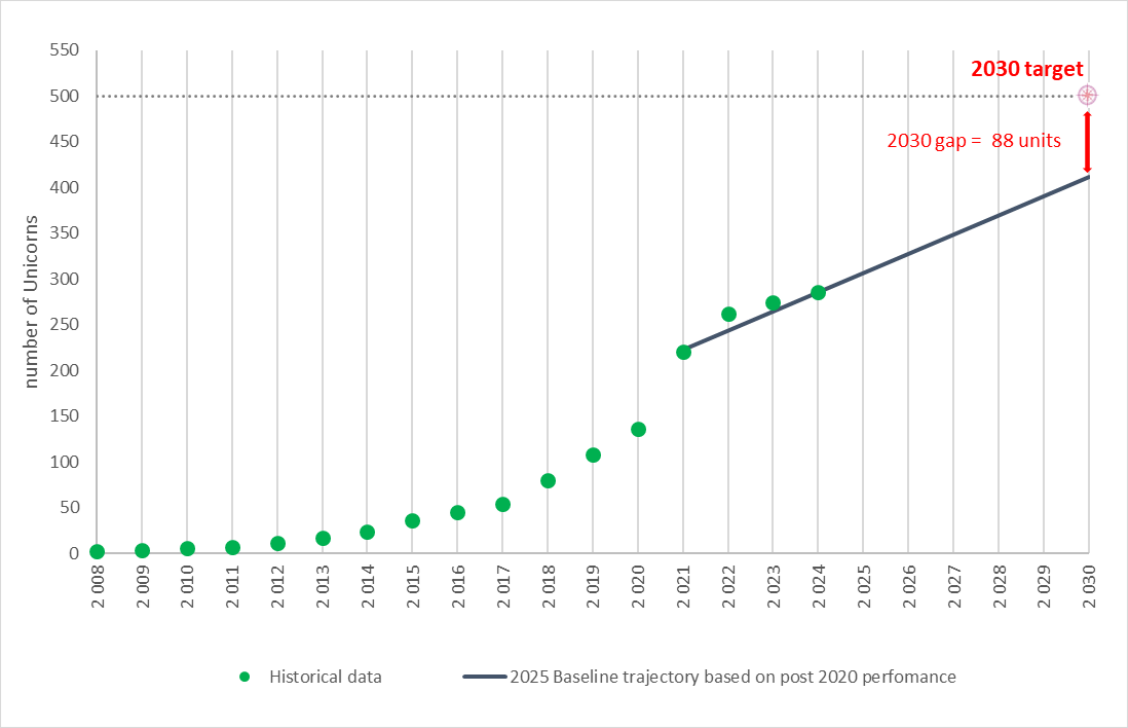
In 2024, the number of unicorns in the EU rose by 12 units (net increase), rising from 274 in 2023 to 286 in 2024 (a year-on-year increase of 4.4%)**.** This corresponds to 52% of the EU's 2030 target. According to the forecast along the revised linear baseline trajectory, **about 82% of the target is expected to be achieved by 2030,** with slightly more than 400 unicorns expected to be active in the EU by then. The target of 500 unicorns is expected to be reached in **2034** if no further actions are taken.

[23] Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, PE/72/2018/REV/1, 2019.

[24]Dealroom, Unicorns, 2025. Available at: https://dealroom.co/guides/unicorns

[25]The Dealroom platform regularly updates the number of unicorns, the dataset used in this document was downloaded on 24/03/2025 and refers to the years from 2008 to 2024 including all possible retroactive revisions. This includes, for example, a new total of 262 for 2022 (it was previously 249) and 274 for 2023 (previously 263). The UK was excluded from the statistics.

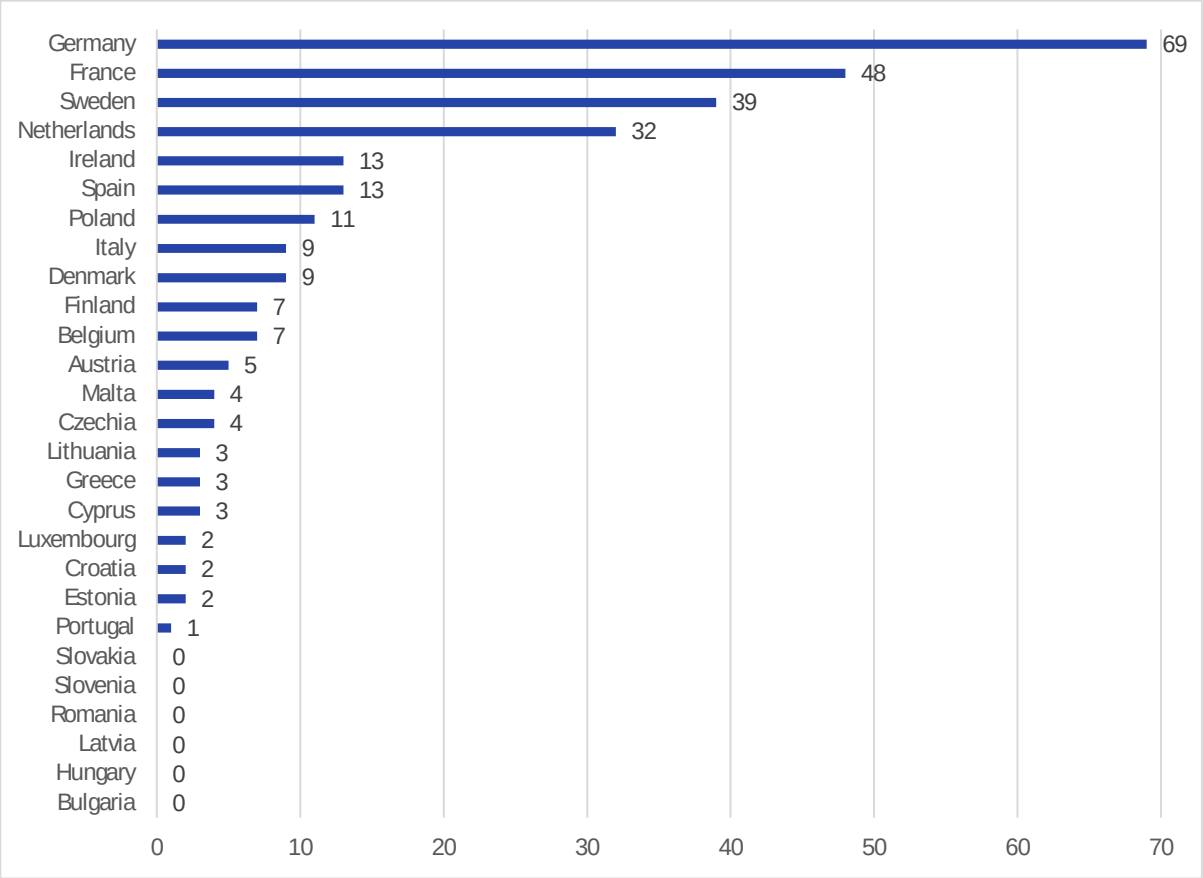
Figure 5: Number of unicorns in the EU. Historical data and revised baseline trajectory



When looking at the data on **unicorns in the EU**, it becomes clear that the strong growth that characterised COVID times, in 2021 and 2022, has slowed down. Moreover, there are significant variations among Member States in the number of unicorn companies. As shown in *Figure 6* below, Germany tops the list with 69 unicorns, followed by France with 48 and Sweden with 39. The Netherlands ranks fourth with 32 unicorns. Conversely, Portugal has only one unicorn, while countries like Bulgaria, Hungary, Latvia, Romania, Slovakia, and Slovenia report none.

On **the global scale the difference in absolute numbers of EU-headquartered unicorns** remains stark, with 286 unicorns in the EU, 397 in China, and 1 681 in the USA at the end of 2024. In percentage terms the EU's 2024 total represented a growth of 4.4% compared to 2023 (slightly lower than the growth 4.7% rate of China). By comparison the growth rate in the US was 6% over the same period.

Figure 6: Number of unicorns, 2024



Source: Dealroom.co

Towards an EU Start-up and Scale-up Strategy

The European Commission is set to adopt an EU Start-up and Scale-up Strategy in 2025, reinforcing its commitment to fostering innovation, competitiveness, and technological leadership. This initiative aligns with the broader objectives of closing the innovation gap between the EU and global competitors, as outlined in key reports such as the Letta Report on the future of the Single Market and the Draghi Report on European competitiveness. The Competitiveness Compass, adopted in January 2025, underscores this Strategy as a flagship action within its first pillar, 'Closing the Innovation Gap'. Addressing financial, regulatory, and administrative barriers that hinder start-ups from scaling into mature, profitable companies is now an urgent priority to prevent their relocation outside the EU. In addition, the Commission is working on a '28th regime' proposal that guarantees one set of rules across the EU making it easier for companies to operate across the EU.

Accelerating Member State actions under national competencies

EU action alone is not enough to address these challenges. Member States, under their national competencies, also have an important role to play to 'raise the floor' for start-ups and scale-ups. There are opportunities at member state level to take action relating to attraction and retention of talent, access to finance, tech transfer policies and public procurement of innovations. Facilitating

this is the Member State-led Europe Startup Nations Alliance[26] (ESNA), that supports Member State innovation policy makers in the sharing and implementation of best policy practices for start-ups. In 2024 ESNA grew its membership from 18 members to 21, reflecting the growing focus of member states on ensuring start-ups have the best framework conditions for growth.

The potential of the Single Market

For innovative companies to emerge and existing ones to scale up, the **Single Market plays a crucial role**. The EU's competitiveness begins within its **Single Market**, which serves 449 million consumers and 31 million active companies, the majority of which are SMEs[27]. Despite its vast economic potential, the Single Market – particularly the Digital Single Market – remains fragmented, leaving approximately a large potential untapped.

This fragmentation results from a complex landscape of national regulations, administrative procedures, and obstacles to data and knowledge sharing. These challenges hinder the efforts of innovative digital technology companies to scale up across borders.

However, it is not just regulations or administrative procedures that dampen growth possibilities for start-ups. A limited number of large online platforms acting as gatekeepers play an important role in facilitating access to important digital services for companies and citizens. In order to foster a more level playing field for small businesses from the EU as well as third countries that use such gatekeeper platforms to reach consumers, the **Digital Markets Act** is now in force and imposes specific obligations and restrictions on these gatekeepers. The DMA is creating significant opportunities to drive innovation in the digital world and enhance fairness and contestability in digital markets (see box below).

Digital Markets Act – Achievements in 2024

The **Digital Markets Act (DMA)**, which became fully applicable in 2024, aims to ensure fair and open digital markets by imposing specific obligations on designated large online platforms – known as **gatekeepers** – that provide core platform services such as search engines, app stores, and messaging services. In 2024, the Commission designated Booking Holdings as a gatekeeper for the provision of **Booking.com** and added Apple's **iPadOS** to the list of designated core platform services, bringing the total covered by the regulation to seven gatekeepers and **24 core platform services**. The Commission also launched six **non-compliance investigations** against Alphabet, Apple, and Meta, and initiated two **specification proceedings** to enable greater interoperability of Apple's software and devices.

To date, the **DMA has demonstrated its tangible and visible impact** by addressing some of the key issues in the digital sector. This impact is illustrated through the examples discussed below.

Choice screens and easier uninstallation: The DMA empowers users to easily switch between various digital services on the gatekeepers' operating system or web browser. For example, Apple removed several sources of friction in the user journey for choosing an alternative web browser and increased the number of software applications for which users can switch the default or that users can un-install. Alphabet also displays an options screen on Chrome, Pixel and over time on all Android devices to enable users to easily select the search engines and web browsers of their choice.

[26] ESNA website: https://esnalliance.eu/.
[27] European Parliament, Deepening the single market in the light of the Letta and Draghi reports, 2024.

Opening up of mobile ecosystems: the DMA opened up opportunities for developers. These developers should be free to decide through which channels they wish to distribute their apps and users should be allowed to access these apps or app stores outside the gatekeepers' app stores. Apple now must allow iPhone and iPad users to install apps by means other than Apple's own App Store, for example by enabling third party app stores and directly downloading apps from the web. This led to a number of third-party app stores being launched in the EU, such as AltStore, Aptoide or Epic Game Store. Alphabet's ecosystem has become even more open. Developers that depend on Apple's and Google's operating systems and stores can now directly contact users, inform them about offers and direct them to purchase in-app features and services outside the app stores of the gatekeepers.

Parity clauses: The DMA also aims to create fairer and more contestable marketplaces. For example, the DMA eliminates barriers that prevent businesses from offering their goods or services through other platforms or direct sales channels at conditions of their choice. As a result, since 1 July 2024, travel services companies (i.e. lodging, car-rental, taxi rides, attractions) in the EU are free to offer different prices and conditions on Booking.com compared to their own direct sales channel, such as their website, or another online platform.

Access to finance

Another essential issue is the **need for substantial development of EU capital markets**. A relative lack of private capital for 'big ticket' investments forces too many EU start-ups to seek late-stage growth capital from venture capital funds outside of Europe, which often leads to them moving their corporate headquarters outside of the EU.

Late-stage **venture and growth capital funds in Europe** is relatively scarce and fragmented in the EU, especially compared to corresponding markets in other jurisdictions. The **Savings and Investments Union**[28] will be crucial to improve how the EU financial system **channels savings to productive investment**, providing a wider range of efficient financing opportunities for citizens and businesses. It will **promote equity investment** in general with a particular focus on **venture capital/growth capital**.

The increasing need for greater simplification

Beyond fragmentation on the Single Market, EU companies face growing administrative burdens due to regulations, particularly in areas like digital, energy, manufacturing, health, and transport. More than half of European SMEs flag such regulatory and administrative obstacles as their greatest challenge[29]. The fast-evolving regulatory landscape, with overlaps and obsolescence of some pieces of regulation designed at a time when digital technologies did not exist are increasingly seen by stakeholders as a barrier to doing and developing business as well as driving innovation.

This also demonstrates that public policies are lacking on effectiveness and responsiveness in fostering the competitiveness of EU enterprises. Leveraging digitalisation is crucial to enable a significant shift in regulatory approach towards less red tape and more innovation. By creating safe spaces for experimentation based on digital tools, regulators can collaborate with various

[28] Savings and Investments Union A Strategy to Foster Citizens' Wealth and Economic Competitiveness in the EU, COM(2025) 124 final.
[29] Draghi, M., The future of European competitiveness, Part A – A competitiveness strategy for Europe, p. 14 2024.

stakeholders including innovative enterprises, to understand emerging technologies, assess potential risks, and develop appropriate regulatory frameworks that balance innovation with consumer protection and systemic stability. The Omnibus packages of simplification measures are designed to address these changes and support the simplification process. The Omnibus proposal aims to streamline and modernise regulatory frameworks across the EU, reducing unnecessary complexities and fostering a more innovative and competitive environment.

As a cornerstone of the simplification agenda the European Business Wallets, building on the EU Digital Identity Wallets, are set to provide a universally accepted digital identity for businesses and streamlined communication channels, facilitating easier access to necessary regulatory and administrative processes, significantly reducing the burden on businesses and enabling them to focus on innovation and growth. Businesses are also able to make use of the full potential of the Single Market, by reducing the complexity of navigating national requirements for communicating compliance and reporting obligations.

1.1.3 Ecosystems and infrastructures to support innovation

The EU stands at a defining moment where digital infrastructure is not just about connectivity but also about resilience, economic security, and global leadership. Despite the urgency, Europe faces significant challenges with gaps in connectivity and computing power. **The EU still lacks pan-European secure and resilient digital infrastructures**. The continent is currently lagging in the deployment of fibre, standalone 5G networks, and edge nodes all of which are essential for providing the necessary backbone for seamless communications, supporting digital services, including critical services, and the connected collaboration in a data- and computing-intensive context.

Both the report on **'The future of EU competitiveness'**[30] and the report on **'The Future of the Single Market'**[31] underscore the need and opportunity for consolidating the European telecoms sector and spectrum policy to free up more space for innovation and growth. **These efforts are vital to address the current surge in AI-driven innovation.** Training new foundation models and building vertically integrated AI applications requires access to **massive increases in computing power and data-storage** as well as **faster, lower latency and more secure digital connectivity**. To meet these needs, a fundamental overhaul of current connectivity architectures is required, ensuring a coordinated management of computing and network resources[32] [33].

Europe's path forward lies in building a strong, secure and highly performant digital ecosystem. Connectivity will be the backbone of Europe's strategic autonomy, ensuring that technological innovation thrives within a competitive Single Market. By prioritising secure and resilient digital infrastructures, the EU can create a platform for sustained economic growth and secure its position as a leader on the global stage.

---

[30] Draghi, M., The future of European competitiveness, Part A – A competitiveness strategy for Europe, 2024.
[31] Letta, E., Much more than a market: Report by Enrico Letta on the Future of the Single Market, 2024.
[32] White Paper: How to master Europe's digital infrastructure needs?, COM/2024/81 final, 2024.
[33] The solution provided by the Connected Collaborative Computing ('3C Network') is also at the basis of the functioning of connected and autonomous vehicles as well as of advanced e-health services, including motoring and care in remote areas.

1.1.3.1 Connectivity

Progress towards the Digital Decade targets

Target: Secure, resilient, performant and sustainable digital infrastructures where all end users at a fixed location are covered by a gigabit network up to the network termination point, and all populated areas are covered by next-generation wireless high-speed networks with performance at least equivalent to that of 5G, in accordance with the principle of technological neutrality.

Source: Broadband coverage in Europe studies for the European Commission by Omdia and Point Topic[34].

Available data points: Fixed VHCN (FTTP & DOCSIS 3.1) 2019 to 2024; FTTP: from 2013 to 2024; 5G: from 2020 to 2024.

2024 data values: VHCN = 82.5%; FTTP = 69.2% 5G = 94.3%[35].

Very High-Capacity Network (VHCN)

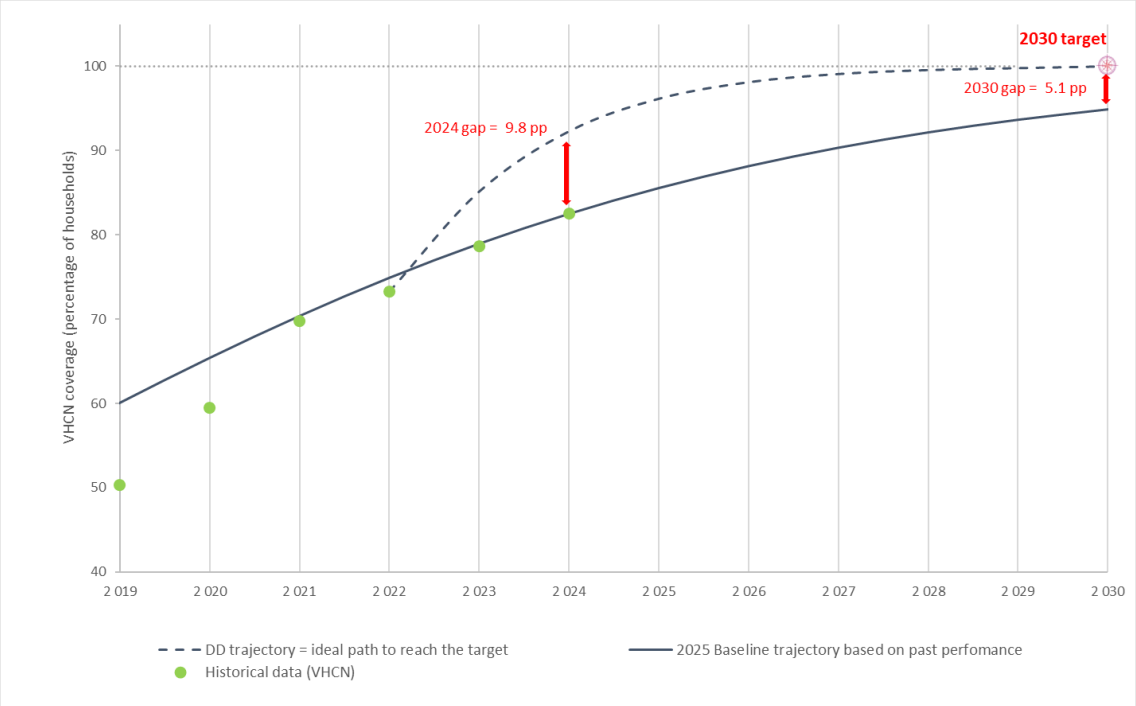
The percentage of households with fixed VHCN connection rose by 3.8 percentage points, from 78.7% in 2023 to 82.5% in 2024. This represents a year-on-year increase of 4.9%.

According to the forecast along the baseline trajectory, 94.9% of the target is expected to be achieved by 2030. In 2024, the value reached by this KPI stood at about 90% the ideal value along the digital decade trajectory (82.5% instead of 92.3%). However, the full target – 100% of households covered – is forecast to be reached only in 2047 if no further actions are taken. The remaining 5% of households still not covered by VHCN will be reached mainly through further FTTP deployments, which require sustained efforts considering that households still not reached by the network are likely to be in the more cost-intensive semi-rural and rural areas, where only 61.9% of households were reached by VHCN in 2024, up from 55.6% in 2023 (+ 11.3%).

[34] Omdia and Point Topic, for the European Commission, Broadband coverage in Europe, 2024.

[35] Note that figures are constantly updated and revised by the National Regulatory Agencies even retroactively. This may cause slight changes of past values with respect to those reported in the '2023 Communication on EU-level trajectories'.

Figure 7: Fixed VHCN coverage in the EU. Historical data, Digital Decade (DD) trajectory and revised baseline trajectory towards 2030

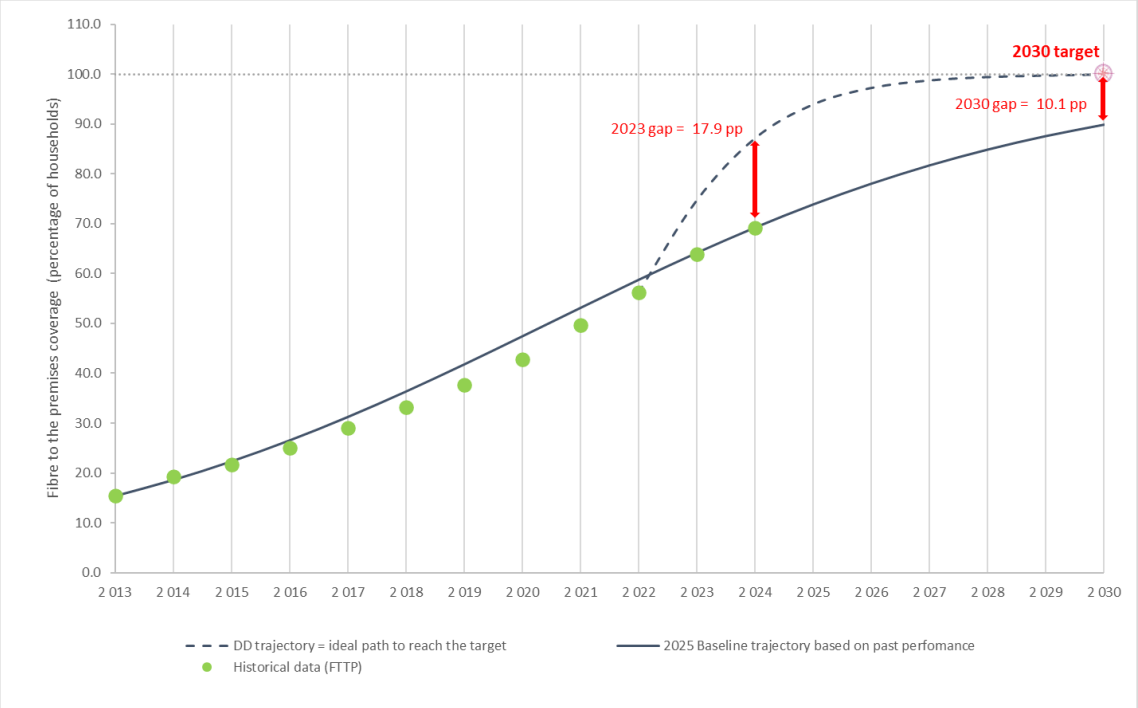


Fibre-To-The-Premises (FTTP)

The percentage of households with fibre connection rose by 5.3 percentage points, from 63.9% in 2023 to 69.2% in 2024. This represents a year-on-year increase of 8.4%.

According to the forecast along the baseline trajectory, 89.9% of the target is expected to be achieved by 2030. In 2024, the FTTP coverage stood at about 80% of the ideal value along the digital decade trajectory (69.2% instead of 87.1%). However, the full target – 100% of households covered – is forecast to be reached only in 2051 if no further actions are taken. Only 58.8% of households living in rural areas were reached by the fibre in 2024, up from 52.6% in 2023 (+ 11.9%).

Figure 8: FTTP coverage in the EU. Historical data, Digital Decade (DD) trajectory and revised baseline trajectory towards 2030



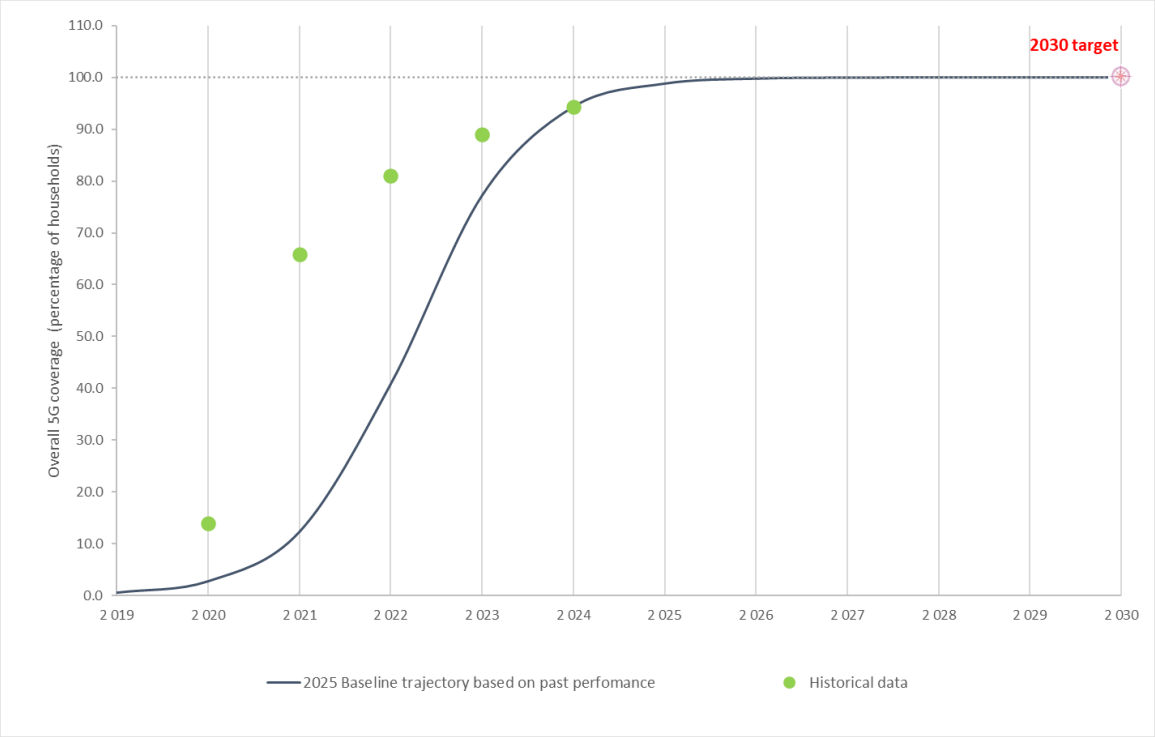
Overall 5G coverage

The percentage of households covered by 5G (all spectrum bands) rose by 5.3 percentage points, from 89.0% in 2023 to 94.3% in 2024. This represents a year-on-year increase of 6.0%.

According to the forecast along the baseline trajectory, 100% of the target is expected to be achieved already by 2027. In 2024, 79.6% of households living in rural areas were reached by 5G coverage, up from 71.1% in 2023 (+ 11.9%).

The percentage of households covered by 5G in the 3.4-3.8 GHz band rose by 16.6 percentage points between 2023 (51.1%) and 2024 (67.7%). This represents a substantial year-on-year increase of almost 32.6%. However, only 26.2% of households living in rural areas were reached by 5G mid-band coverage in 2024, up from 15.9% in 2023 (+ 65.1%).

Figure 9: Overall 5G roll-out in the EU, historical data and revised baseline trajectory towards 2030



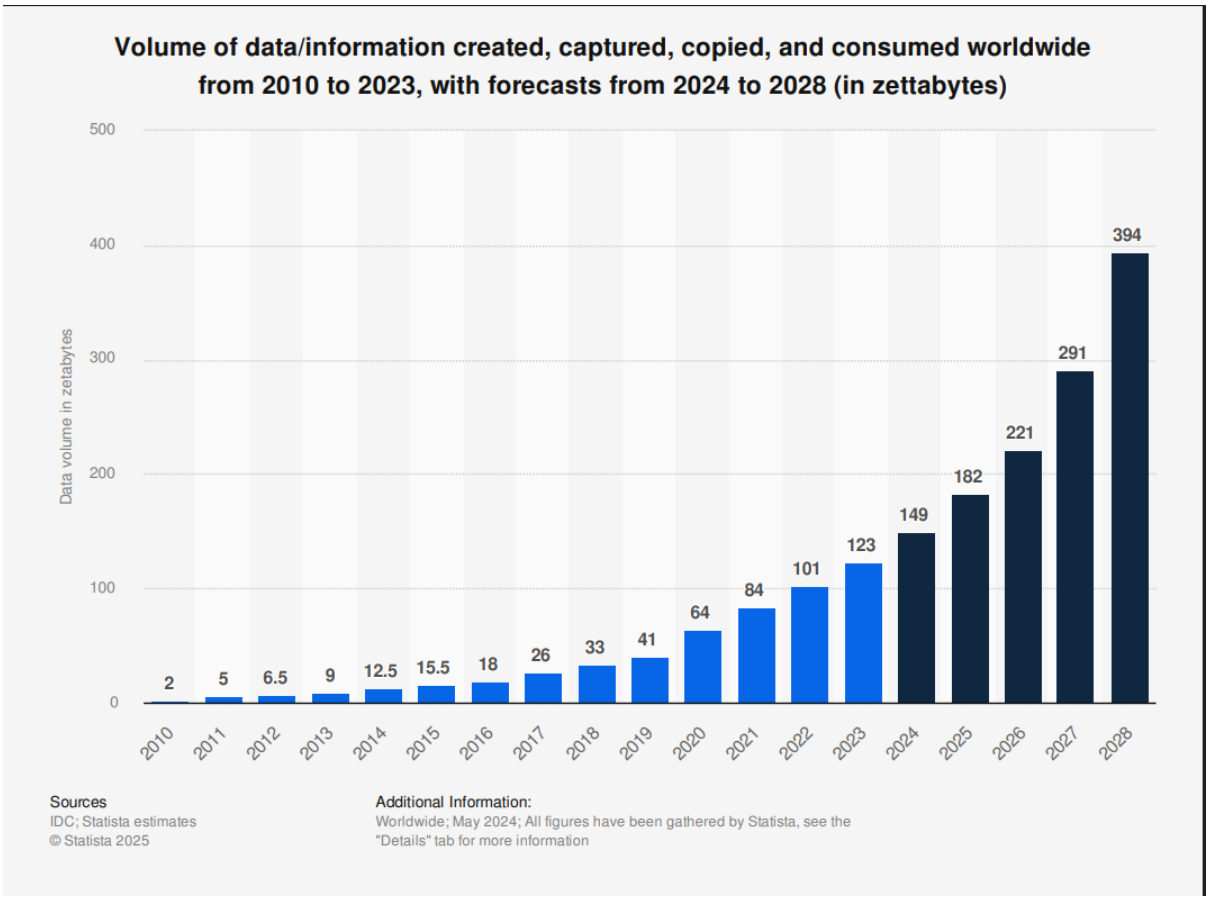
Take-up indicators show a steady increase in high-speed internet subscriptions. In 2023, 65.90% of fixed broadband subscriptions were at speeds of 100 Mbps or higher, rising to 71.88% in 2024, with a growth rate of 9.1%. For subscriptions at speeds of 1 Gbps or higher, the percentage was 18.47% in 2023, increasing to 22.25% in 2024, marking a growth rate of 20.5%. The number of 5G SIM as share of the population also saw significant growth, from 21.70% in 2023 to 35.56% in 2024, with a growth rate of 63.9%.

An integrated policy approach to connectivity

In an increasingly interconnected world, approaching connectivity as a series of isolated technological domains–space systems, submarine data cables, fixed networks, and mobile infrastructure–no longer reflects the complexity of modern data exchange. Today, data traverses these infrastructures seamlessly: a user accessing cloud-based services from a mobile device may rely on local 5G connectivity, terrestrial fibre backbones, submarine cables spanning continents, and satellite relays. This interdependence creates a tightly woven system in which disruption or underinvestment in one component can undermine the performance, resilience, and security of the whole.

The acceleration of latency-sensitive and mission-critical applications–such as autonomous vehicles, remote surgery, and immersive digital environments–further underscores the need for a cohesive, globally optimised infrastructure. Emerging technologies like edge computing, AI-enabled networks, and the proliferation of connected devices (IoT) are eroding traditional distinctions between network layers. Future infrastructure must not only accommodate exponentially growing data volumes–now estimated to amount to close to 400 zettabytes in 2028 (cf. illustration below) but also ensure adaptability, robustness, and geographic reach.

Figure 10.Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2023, with forecasts.



Each layer of this infrastructure contributes a distinct yet interdependent function: submarine cables remain the backbone of international data exchange, carrying more than 99% of international data traffic; satellite systems extend coverage to remote or disrupted regions and offer redundancy; fixed networks deliver high-capacity throughput; and mobile networks provide critical last-mile access.

Such future proof, resilient networks are a precondition for the digital transformation and competitiveness of key European sectors and for the full potential of the data economy to be realised. This redundancy and technical integration of alternative networks is equally vital from a security standpoint, as services requiring ultra-low latency and real-time reliability demand distributed, fail-safe networks.

Yet, fragmented governance and planning can create systemic vulnerabilities or gaps in capacity forecasting, inconsistent cybersecurity frameworks, and limited resilience in crisis scenarios. The global threat landscape continues to intensify; in 2024 organisations faced an estimated 600 million cyberattacks per day, exposing the vulnerabilities of both digital and physical infrastructure, from submarine cable sabotage to satellite interference and mobile network intrusions. Only a unified, cross-domain approach can enable the deployment of coherent security standards and robust operational continuity.

Beyond performance and resilience, a comprehensive approach is increasingly essential to address shared structural challenges related to strategic autonomy and global competitiveness. All layers of connectivity are exposed to geopolitical risk and supply chain dependencies. The EU, for instance, remains heavily reliant on non-European satellite constellations; the Russian war of aggression

against Ukraine highlighted this dependence, as military and civilian communications were critically tied to the availability of the privately operated Starlink system. Similarly, Europe's access to major cloud services – dominated by U.S. providers such as Amazon, Microsoft, and Google, which together account for over 70% of the EU market – is largely dependent on transatlantic submarine cables[36]. This creates potential vulnerabilities in the event of geopolitical tensions or transnational service disruptions.

In parallel, the global competition for leadership in next-generation networks (5G and 6G), semiconductor fabrication, and cloud infrastructure underscores the strategic value of end-to-end control over digital connectivity. Without an integrated approach – ranging from orbital assets to terrestrial infrastructure – regions risk losing influence over critical data flows, technological innovation, and the capacity to uphold sovereign decision-making in the digital realm. In this context, connectivity is no longer a purely technical issue, it is a foundational pillar of economic strength, digital independence, and geopolitical influence.

With this in mind, the EU aims to foster a vibrant community of European innovators advancing the development of integrated connectivity and collaborative computing infrastructures, as described in the 2024 White Paper on "How to master Europe's digital infrastructure needs". To reach this goal, and ensure the economic security of its network infrastructures, the EU needs to enhance research efforts and multi-disciplinary collaboration across its Member States. It also needs to improve access to finance for EU actors, including by coordinating public and private investments effectively.

In parallel, significant efforts are ongoing to scrutinise the regulatory framework for electronic communication networks, in order to make sure that it is fit for purpose to deliver the required innovation and investments. At the same time, a part of EU level public funding is adjusted to these needs too, in particular to support 5G deployments coupled with innovative use cases and to reinforce the resilience, redundancy and security of core networks, as described below.

Working towards a Digital Networks Act

As outlined in the 2024 White Paper on "How to master Europe's digital infrastructure needs", a key focus is the creation of 'Connected Collaborative Computing' Networks ('3C Networks'). This ecosystem will facilitate the creation of end-to-end integrated infrastructures and platforms for telco cloud and edge, which could be used to orchestrate the development of innovative technologies and AI applications for various use cases.

On the regulatory side, an innovation and investment-friendly framework is indeed required not only to realise this vision, but also to achieve the ambitious digital infrastructure targets for the Digital Decade by 2030.

As indicated in the communication 'A Competitiveness Compass for the EU', the Commission is working towards a future Digital Networks Act (DNA), to be proposed by the end of 2025, which aims to improve market incentives to build the digital networks of the future, reduce burdens and compliance costs for businesses, making it easier to operate, and thereby improve digital connectivity for all end-users.

[36] Synergy Research Group, European cloud providers continue to grow but still lose market share, 2022.

As the Commission's 'Work Programme 2025' stresses, the DNA will facilitate cross-border network operation and service provision, enhancing industry competitiveness and improving spectrum coordination. To achieve these objectives, the DNA will create a more integrated Single Market for connectivity, driving further harmonisation and reducing fragmentation across Member States by simplifying processes, and enabling smooth cross-border operations. It will also focus on addressing emerging cross-border challenges, including data privacy concerns, and deliver more clarity on issues such as quality-based services and the Open Internet guidance on specialised services.

Furthermore, the Commission is considering measures to expedite the transition to energy-efficient fibre networks by phasing out copper by 2030, aiming to incentivise deployment while preventing competitive distortions. National Regulatory Authorities (NRAs) will play a crucial role in monitoring the migration process, setting clear timelines, and preventing practices that could undermine competition.

On the public funding side, the creation of the 'Connected Collaborative Computing' Networks is prepared via the set-up of large-scale pilots under Horizon Europe as well as under the Connecting Europe Facility, while a possible new Important Project of Common European Interest (IPCEI)[37] in the computing infrastructure is being discussed.

In particular, the second CEF Digital work programme for 2024-27, adopted in October 2024, builds on the results of the first work programme (2021-23) and reflects evolving policy priorities. It makes a further EUR 205 million available for 5G Large Scale Pilot Projects, by merging the 5G Corridors and 5G for Smart Communities into a single topic. The aim of this new concept of 5G large scale pilots is to integrate 5G standalone system deployments with edge cloud capabilities and with vertical use cases, in order to ultimately stimulate innovation and take-up across Europe. By selecting excellent and highly replicable and scalable projects, CEF (the Connecting Europe Facility) aims to foster a seamlessly connected and secure European digital infrastructure that supports industrial transformation and valuable societal applications alike.

The first Work Programme is progressing with EUR 221 million invested so far in 66 best practise projects, EUR 128 million for 5G Smart Communities and EUR 93 million for 5G Corridors. Several ongoing projects have already integrated 5G standalone with edge cloud capabilities, in order to support applications such as connected and automated mobility, virtual learning environments, remote healthcare, border control, and smart agriculture.

Two examples of projects (currently under implementation)

High Connectivity via 5G (HI5): This project offers 5G connectivity and enables smart traffic management and surveillance as well as connectivity for Services of General Economic Interest (SGEI) across the Toulouse metropolitan area. The initiative builds on the Métropole's large existing data centre infrastructure, high points and optical fibres, to create a resilient and independent 5G private infrastructure at low operating costs.

5G NETC: the project aims to improve cross-border network service continuity for established services and adopt 5G infrastructure in public environments to support new 5G services and applications. The goal is to enable applications and services for connected and automated mobility on road and 5G-enabled Future Railway Mobile Communication Systems (FRMCS) use case solutions

[37] IPCEIs are State aid instruments, funded by Member States under EU State aid rules.

and their introduction. 5G NETC covers a 3 354 km length of transport path between SE-FI-DK-NO-LV, and benefits from a EUR 15 million EU grant.

Ensuring that spectrum needs for future connectivity are met

Despite the delays beyond legal deadlines, the assignment of the three 5G pioneer bands has progressed across the EU and reached 74% on average (February 2025). The 3.6 GHz primary 5G band has been allocated in all EU-27, although in some Member States only partially. Market demand has been staggered for the 26 GHz pioneer band, which has resulted in fragmented assignment (of at least 1 GHz) in 12 Member States, or 44% on EU average. The 700 MHz pioneer band has been assigned in 25 Member States.

While the implementation of the 5G spectrum roadmap is almost complete with the harmonisation of the 42 GHz band and the ongoing harmonisation of the 3.8-4.2 GHz band targeting mainly vertical applications, the EU is set to develop a spectrum roadmap towards 6G. In this regard the Radio Spectrum Policy Group (RSPG), following the adoption of its Report on a 6G Vision is starting work on a 6G spectrum roadmap. This is correlates with the topics of future use of the upper 6 GHz band and the sub-700 MHz band as well the forthcoming RSPG Opinion on WRC-27.

Another major related work item of the RSPG is aiming to define an EU-level policy approach to satellite Direct-to-Device (D2D) connectivity and related Single Market issues. Those deliverables are essential inputs to the inception of a comprehensive future EU spectrum roadmap to address wireless broadband and sectoral needs as well as the impact of network convergence.

Standard setting for 6G

The global race for 6G standardisation demands a proactive EU role. From a European perspective, it is crucial that EU policies and priorities shape the global standardisation landscape, ensuring that European companies remain well represented even as new stakeholders, particularly vertical industries, join the dialogue.

Whilst the 5G standardisation process is still ongoing, the EU has actively contributed to shaping the future of mobile connectivity. Notably, hundreds of industry contributions to the 3GPP originate from EU-supported projects under the 5G PPP initiative and the SNS JU.

EU action for 2025 is focused on fostering global industry standards under EU leadership for key 5G/6G technologies, including radio access and core networks, and for innovative network architectures. This is being achieved through the active exploitation of EU-funded research results in major international standardisation bodies such as 3GPP, ITU, and ETSI.

In addition, ensuring that 5G/6G standards are compatible with innovative vertical use cases and that adequate spectrum is available will require broader participation from industries and sector-specific standards-developing organisations.

An inclusive standardisation process is essential to address the divergent market needs across regions, and the European Commission remains committed to ensure that all relevant use cases are represented. To this end, the inception workshop organised by 3GPP in South Korea in March 2025 started officially the 6G standardisation process.

Open RAN

Open Radio Access Network (RAN) can potentially represent an opportunity to foster a more diversified and thus more competitive vendor landscape. By opening the main components of the RAN to a wider set of suppliers, Open RAN can promote innovation and cost efficiency.

On 4 December 2023, Ericsson and AT&T announced a USD 14 billion strategic agreement for a five-year cloud-native open network development based on Open RAN. Furthermore, Nokia and Deutsche Telekom (DT), have begun to deploy a multi-vendor Open RAN network with Fujitsu in Germany. Other recent significant partnership announcements include those between Ericsson and Telefonica, Nokia and DT and Nokia and Vodafone. Finally, Orange and Vodafone agreed to build an Open RAN with RAN sharing in rural parts of Europe where they both operate mobile networks. The initial commercial deployment in a rural area near Bucharest, Romania, constitutes a real-life experience of the new operational model, integrating multi-vendor hardware and software. All these developments suggest that EU vendors intend to be active across all 5G segments.

Open RAN advocates also claim that Open RAN can reinforce network security. However, the joint report by EU Member States in 2022 on Open RAN's cybersecurity challenges remains a critical reminder that, despite its potential, Open RAN still lacks maturity and poses significant security risks.

Presenting its Mobile Economy Europe 2025 report, the GSMA highlighted two elements relative to Open RAN, confirming the cybersecurity challenges, due its large attack surface and the mitigated openness of the network, as it is often the case that operators choose a sole vendor for Open RAN provision.

The Commission is monitoring developments[38], with the objective of consolidating Europe's position in the telecom supply chain, while accelerating advanced 5G network deployment. In this context, Open RAN could be seen as another opportunity to reinforce the EU supply ecosystem. To this end, the Commission is supportive of the inclusion of Open RAN specifications in the 3GPP process.

Working to develop and integrate space connectivity

The satellite market is undergoing significant transformation, driven by decreasing costs for space launch and satellite manufacturing. Satellites are increasingly seen not only to provide broadband connectivity to underserved areas – albeit not a full substitute to fibre optic connectivity – they are becoming an essential component of a secure and resilient converged terrestrial/non-terrestrial network.

This trend has been enabled by the development of satellite constellations in non-geostationary orbits (NGSOs), particularly low earth orbits (LEOs) which facilitate low-latency exchange of data at a higher rate and enable, alone or in combination with satellites in higher orbits, a multitude of use-cases.

Moreover, the convergence and integration of non-terrestrial-network (NTN) and terrestrial networks will become increasingly prevalent thanks to the latest 3GPP Standard releases, which include the integration of satellite connectivity for 5G and for 6G in the future. This will help supplement terrestrial mobile connectivity using satellites (satellite direct-to-device, i.e. D2D) and make it more resilient and secure, thanks to advanced encryption features. As a result, satellite

[38] European Commission, 5G Observatory, 2025.

operators are both competing with and partnering with mobile network operators (MNOs), as evidenced by several recently announced MNO/satellite collaborations.

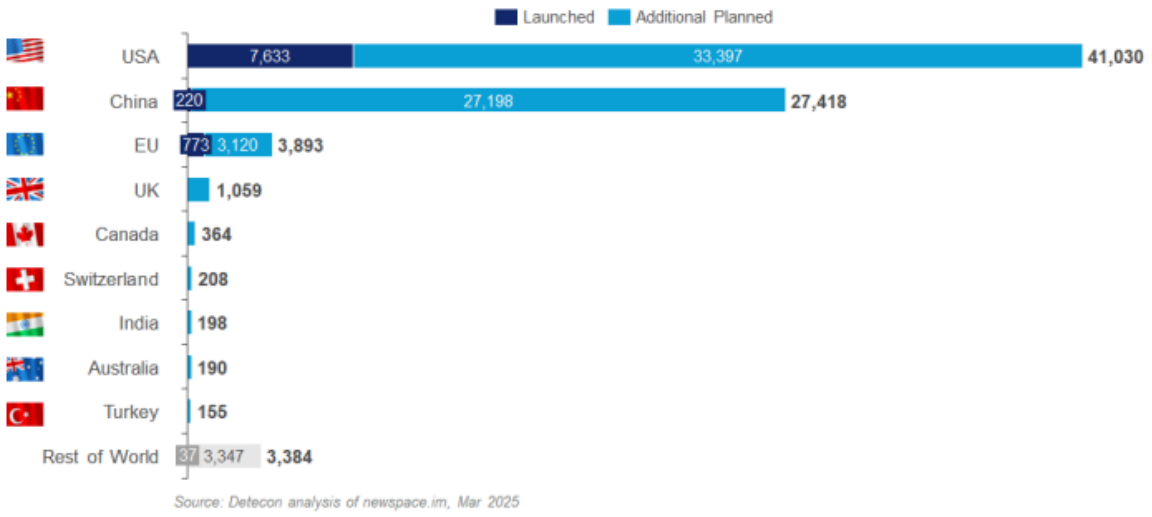
The EU is actively regaining strategic presence in space. A cornerstone of this effort is IRIS², the new EU multi-orbit satellite constellation for secure connectivity. In December 2024, the European Commission and the SpaceRISE industry consortium, comprising the three major EU satellite operators, signed a 12-year concession contract for the design, development, and operation of IRIS². Once operational in 2030, IRIS² will consist of 292 satellites in medium earth orbit (MEO) and low earth orbit (LEO), providing secure connectivity services to EU institutions, private companies, and citizens, as well as high-speed broadband to eliminate connectivity dead zones. Europe's largest LEO constellation, Eutelsat's OneWeb, has 661 satellites launched, with a signed order with Airbus to add a further 100 satellites in future.

Despite this progress, IRIS² represents only an incremental step in the EU's satellite capacity, with Europe's current 3 893 launched and planned satellites far behind the US (7 633 launched and an additional 33 397 planned satellites) and China (220 launched and an additional 27 198 planned satellites), confirming the extremely ambitious expansion plans for both US and China in the coming years[39]. On the regulatory side, the Commission continues its work to develop a common approach for the satellite constellations that will provide services in the EU. In 2024, the Commission requested the Radio Spectrum Policy Group (RSPG) an opinion on satellite constellations access to the EU market and satellite D2D that will be published in June 2025. Additionally, the EU is exploring the potential of the EU harmonised 2 GHz mobile satellite system (MSS) frequency band, which will become available for reassignment in 2027, as a strategic tool to support its ambitions in the space market. The RSPG published an opinion in February 2024 and a study is being conducted by the European Commission on the implementation of the current regulatory framework for MSSs, the satellite connectivity market and forward-looking regulatory issues and scenarios.

By investing in secure, resilient, and competitive satellite infrastructure, the EU is ensuring that space connectivity remains a cornerstone of its technological sovereignty, reinforcing Europe's security, economic resilience, and leadership in next-generation telecommunications by fostering innovation.

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

Figure 11. Broadband Internet, D2D and IoT satellite constellations in terms of total number of launched and planned country/region[40]



Source: Detecon International GmbH

<u>Submarine cables: working towards secure and resilient backbone networks</u>

Submarine data cables are the backbone of global digital communication, carrying over 99% of international data traffic, making their security and resilience a top priority for the EU. Enhancing cable security is fundamental to the EU's goals of safeguarding its digital sovereignty, boosting economic resilience, and mitigating potential vulnerabilities that could be exploited by geopolitical adversaries.

In response and following the 2024 White Paper on 'How to Master Europe's Digital Infrastructure Needs' and the 'Recommendation on Secure and Resilient Submarine Cable Infrastructures,' the European Commission established an Expert Group comprising Member State authorities and the European Union Agency for Cybersecurity (ENISA), which held its third meeting on 12 March 2025. This Group is responsible for monitoring security risks, sharing best practices, and coordinating resilience measures across the EU.

In February 2025, the European Commission and the High Representative adopted the EU Action Plan on Cable Security, a major step toward strengthening Europe's submarine cable infrastructure. This plan adopts a comprehensive resilience cycle approach, focusing on prevention, detection, response, recovery, and deterrence, including: prevention through coordinated risk assessments and mitigation; detection via enhanced surveillance and real-time monitoring; response by establishing rapid-response mechanisms and improving the EU-level crisis framework; recovery through ensuring repair vessel availability, facilitating spare part stockpiling, and setting up an EU Cable Vessels Reserve; and deterrence via legal, diplomatic, and strategic actions against perpetrators of cable disruptions and hybrid threats, while fostering 'cable diplomacy' with global partners. These

[40] Please note that these figures are indicative and do not account for the complexities of multiple shareholders from different countries, unless it is close to a 50/50 split. Moreover, these figures exclude some claims and announcements. Finally, counting satellites may also not be the most accurate metric, as it does not account for weight. Comparing kilograms in orbit is probably a more meaningful metric, should it become available.

initiatives are expected to launch throughout 2025 and 2026, underscoring the EU's dedication to safeguarding its critical infrastructure.

On the funding front, CEF Digital has been supporting since 2021 the deployment of new or significant upgrades of existing backbone networks, including submarine cables, within and between Member States and between the EU and non-EU countries. To date, 51 Digital Global Gateways projects have been signed for a total of EUR 420 million.

These projects significantly contribute to boosting global connections between **Europe and Africa** (e.g. the Medusa Africa or Canalink-Morocco projects), the **Middle East** (e.g. the BlueMed East project) and **Asia** (Arctic connectivity), as well as reinforcing connections between Member States in the Mediterranean, the Atlantic, the Baltic Sea and Continental Europe (including Central and Eastern Europe). These projects also support connectivity in **Outermost Regions** and **Overseas Countries and Territories**, like in the Pacific Ocean (e.g. the NUANUA project), the Caribbean (e.g. the BCA project), the Canary Islands (e.g. the PENCAN-X project) and the Azores-Madeira area (e.g. the Atlantic CAM project).

The **second CEF Digital Work Programme 2024-2027,** adopted in October 2024, has made an additional EUR 542 million available to co-fund backbone connectivity projects, bringing the EU's total investment in these critical infrastructures over the current financial framework to nearly EUR 1 billion.

A significant part of the CEF Digital resources will continue to support the deployment of new backbone networks, in particular, submarine cables within and between Member States and between the EU and non-EU countries. Thus, contributing to the increased coverage, capacity, resilience and security of EU's digital communications infrastructure. Not least, CEF Digital will support quantum communication infrastructure by co-funding cross-border links between national quantum communication networks and the deployment of optical ground stations for interconnections with the EuroQCI's space component. This will complement the national QCI projects, as well as the overarching actions to develop European quantum communication technologies funded under the 2021-22 DIGITAL work programme.

1.1.3.2 Semiconductors

Progress towards the Digital Decade target

Target: Secure, resilient, performant and sustainable digital infrastructures where the production, in accordance with Union law on environmental sustainability, of cutting-edge semiconductors in the Union is at least 20% of world production in value.

Source: Study in progress by the International Data Corporation.

Available data points: from 2019 to 2023.

2024 data value (estimate): 10.5% of the global market share by value.

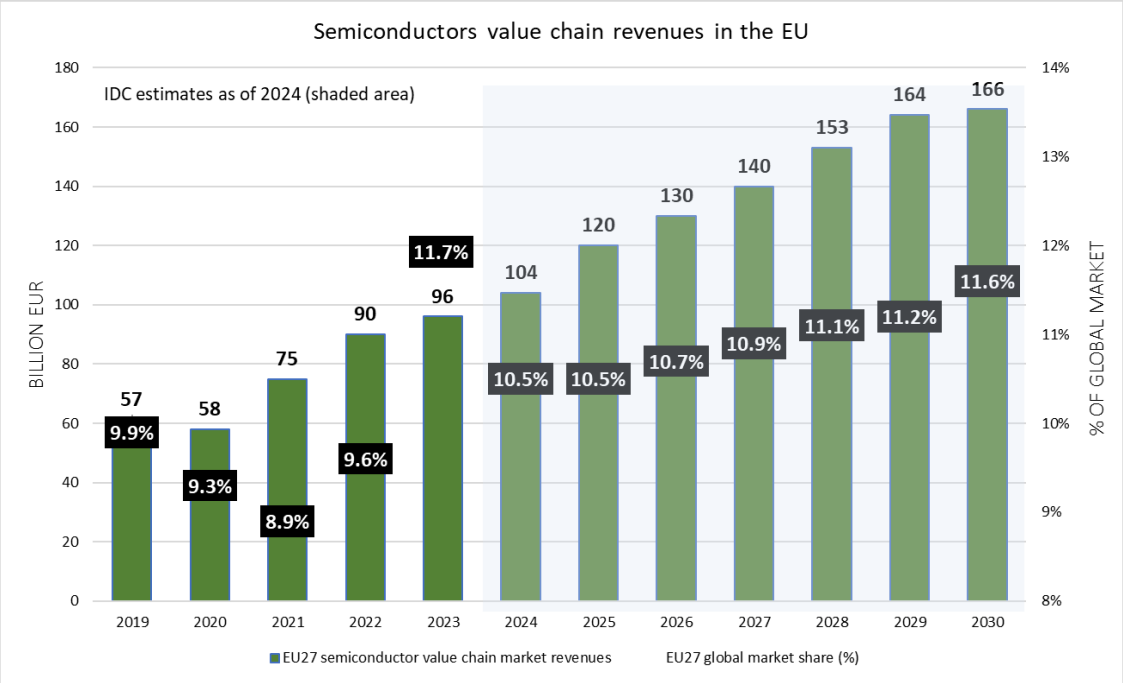
The European Union has set ambitious goals for the digitalisation of its economy where the development of the semiconductor industry is a key component of the strategy.

The historical evolution of the EU semiconductor value chain revenues has experienced a steady increase from EUR 57 billion in 2019 to EUR 104 billion in 2024, as shown in the figure 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 166 billion in 2030.

According to an ongoing study by the International Data Corporation (IDC), the 11.7% EU's share of global value chain revenues in 2023 was due to strength from equipment, automotive and industrial companies as they fulfilled long lead time products. Inventory corrections and the high growth of the global market led the EU's market share to a forecasted 10.5% in 2024. It is worth nothing that the EU's share is projected to constantly increase again in the coming years pulled by the steady growth of the EU's value chain revenues. This relative increase will occur despite the strong growth of the global market revenues now projected to pass EUR 1.4 trillion in 2030. The steady increase of both the EU's semiconductor value chain revenues and the relevant EU's share confirm the effectiveness of EU policy for the sector, where the digital transition and the global demand for semiconductors rapidly accelerate with fierce competition from other regions all over the world.

The projections indicating that the global semiconductor market will exceed EUR 1.4 trillion by 2030, effectively more than doubling its value over the decade, implies that the EU's semiconductor revenues must more than quadruple from its current value if its Digital Decade target is to be achieved by 2030.

Figure 12: EU semiconductor value chain revenue and share versus the global market. Values are estimated as of 2024



Source: International Data Corporation

To address this challenge, the EU has been pushing its main policy interventions in the sector. The European Chips Act has established a framework to attract investments from major semiconductor manufacturers into a first-of-a-kind for EU facilities, with the first seven projects announced already exceeding EUR 30 billion in investments and with further promising projects in the pipeline; the approved Important Project of Common European Interest on Microelectronics and Communication Technologies (IPCEI ME-CT), building on the first IPCEI on microelectronics, brings together 14 Member States and 56 companies, channelling a combined total of around EUR 20 billion from both private and public sources into 68 collaborative projects across multiple countries; furthermore, proposals for new IPCEI candidates in the area of advanced semiconductor technologies, as well as

other topics in the digital field such as AI and computing infrastructure, are currently in the design phase.

The IDC's study takes into account the impact of such policy interventions and investments, whose tangible effects are expected to become apparent and further positively impact the market figures in the second half of the decade.

For Europe to globally compete in the sector, doubling down on investments and continuing its commitment on the leading value chain areas such as semiconductor equipment, chips design, analog semiconductors, sensors, photonics, while entering the computing and AI silicon markets is mandatory. The progress made in the EU has been positive and has become a solid foundation that will continue to encourage change and innovation not just from a technology perspective but also in proving a framework that drives sustainable development, and businesses plan across companies in the region.

1.1.3.3 Cloud & edge infrastructure

Progress towards the Digital Decade target

Target: Secure, resilient, performant and sustainable digital infrastructures where at least 10 000 climate-neutral highly secure edge nodes are deployed in the Union, distributed in a way that guarantees access to data services with low latency (i.e. a few milliseconds) wherever businesses are located.

Source: Edge Observatory

No available observed data points

2024 data value (estimate): 2257.

The **Edge Observatory** for the Digital Decade reported that a total of **2 257 edge nodes** were deployed across the EU in 2024, reflecting a single-year increase of **1 072 new nodes** compared to 2023.

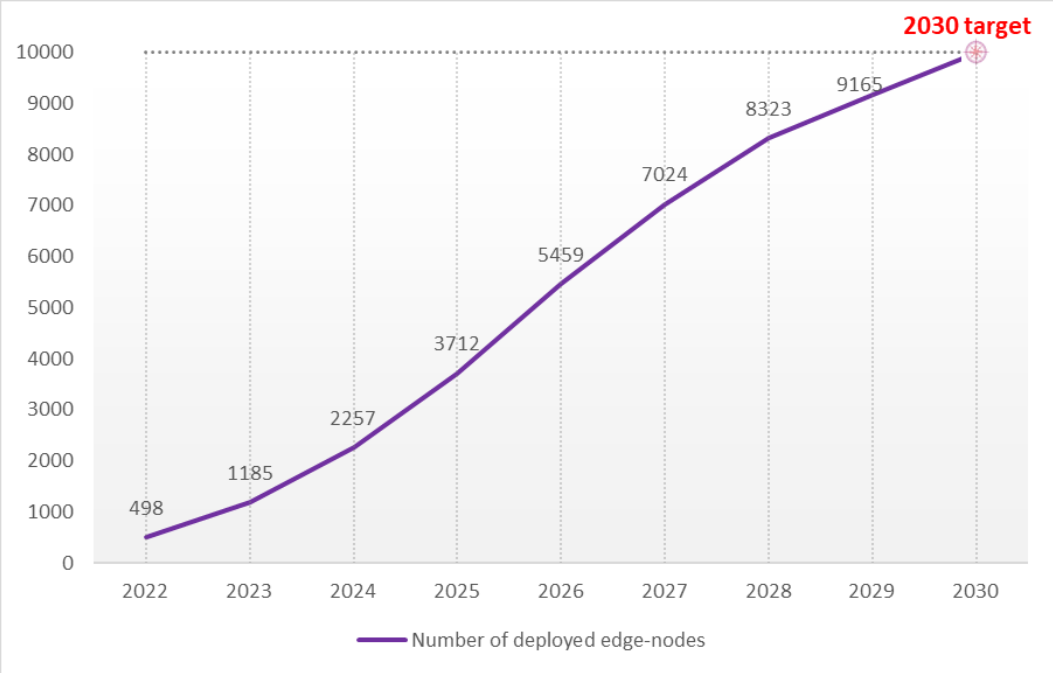
The edge nodes trajectory is based on the data prepared by the Edge Observatory study[41]. The trajectory began modestly in 2022, with 498 nodes deployed. The deployment has continued to gather momentum in 2024, marking the start of a more aggressive scaling phase that aims to extend connectivity to broader areas, including rural and underserved regions.

2025 represents a pivotal moment in the deployment trajectory, in which it is expected the most substantial single-year increase of 1 455 new nodes. As the deployment enters 2026, the pace is expected to remain strong pushing the total to 5 459 nodes. However, as the infrastructure matures, the rate of new deployments is expected to moderate slightly in 2027, with 1 565 new nodes, reaching a cumulative total of 7 024 nodes.

The trajectory shows a gradual tapering off in new deployments in 2028 and beyond, as the network nears completion. By 2030, the final push adds 835 nodes, culminating in the target of 10 000 nodes. This final phase ensures that the network is fully operational and capable of supporting a wide range of digital services and applications across the EU.

[41] European Commission, Edge observatory for the digital decade – monitoring the deployment of edge nodes, 2024.

Figure 13: Edge node estimated deployment (EU projection to 2030). The edge node trajectory is based on findings of the Edge Observatory study (https://digital-strategy.ec.europa.eu/en/policies/edge-observatory)



The density of edge nodes across the EU reveals varying levels of deployment across member states. France, Germany, Italy, and Spain are at the forefront of Edge node deployment. As part of their efforts, these leading Member States should prioritise the deployment of edge nodes that support high-demand applications. Moreover, these member states could benefit of edge deployments targeted for AI data processing and integration with future digital infrastructures. Member States in which edge deployments remain less widespread (Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Greece, Hungary, Latvia, Lithuania, Luxembourg, Malta, Portugal, Romania, Slovakia, and Slovenia) are encouraged to promote experimentation and target deployments, with particular emphasis on AI-driven applications to showcase the value of edge computing and lay the groundwork for larger-scale implementations.

In this context, today's edge node deployments are mainly addressing the critical need of accessing real-time data, with 20% of organisations already using such solutions extensively and 42% planning to adopt them. Over time, AI and machine learning applications in business use cases indicate a **promising future adoption rate of edge nodes** at 54%. This underlines the transformative potential of artificial intelligence and machine learning in driving business innovation, decision support, and monetisation of edge solutions[42].

The relevance of edge computing in view of exploiting the potential of AI

Progress in AI is sustained by advances in three main areas: algorithms, data and compute infrastructure. For the latter, researchers estimate the amount of compute utilised to train leading AI systems has expanded by 350 million times over the past 13 years[43] and is growing at a pace of 4.6

[42] European Commission, Edge Observatory for the digital decade – monitoring the deployment of edge nodes, 2024.
[43] Lennart Heim, Markus Anderljung, Emma Bluemke, Robert Trager, Centre of the Governance of AI, Computing Power and the Governance of AI, 2024.

times per year[44]. These figures, offer an understanding that AI's full potential can only be reached if computer infrastructure and software are available to train and use AI models at scale. According to the OECD, a lack of access to the necessary infrastructure and software can cause compute divides to emerge or deepen, undermining AI's productivity gains and competitive advantages[45].

In this regard, different types of AI processes pose different requirements that compute infrastructures need to meet to execute these processes. The state-of-the-art trend in generative AI and large language models is heavily reliant on extremely high-performance processing, storage of large data sets and advanced scalability means. This is despite algorithmic and software enhancements in pursuit of reducing the computing power needs. These elements are solely available in high concentrations of computing power, made accessible through cloud services. Next to this, the inference of generative AI and large language models, along with fine-tuning and execution of predictive AI processes, is suitable for edge computing environments and the compute capacity available in edge nodes. The reason is that these processes obtain enough computational resources by relying on general purpose hardware enriched with lower-end hardware accelerators, for instance, in GPUs, smart network interface cards (smartNICs) and field programmable gate arrays (FPGAs) which are commonly available in edge nodes.

The requirement to gather, process, and transmit massive amounts of data to the central cloud is a roadblock for AI use cases that require low latency. **Edge computing has the potential to act as a critical component for AI inference** closer to where data are generated as part of a distributed edge and cloud environment for AI. This encompasses multiple use cases like video observation and analysis and asset/equipment monitoring, tracking, or performance optimisation to cite just a few[46]. Edge computing enables more immediate AI processing of the massive data volumes of generated at the edge, the intelligent interpretation of this data in minimal processing times (milliseconds), while providing a more secure processing environment and lowering data transmission costs and network congestion.

Ongoing policy developments: the IPCEIs and the Cloud and AI Development Act

Following its approval on 5 December 2023, the activities of the **IPCEI Next Generation Cloud Infrastructure and Services (IPCEI-CIS)** kicked off in March 2024 with a number of R&D&I projects and first industrial deployment that will last until December 2031 (as the projects of different companies have different duration, this is the latest end date of a participating project) (see box below).

Progress on the IPCEI Next Generation Cloud Infrastructure and Services (IPCEI-CIS)

A total of 19 companies from seven member states (France, Germany, Hungary, Italy, the Netherlands, Poland, and Spain) are participating in this IPCEI. The IPCEI CIS will put Europe on the path to the cloud infrastructure of the future. To this end, the seven participating Member States are providing up to EUR 1.2 billion in public funding, unlocking an additional EUR 1.4 billion in private investments.

---

[44] EPOCH AI, Notable AI models, 2025.
[45] OECD, A blueprint for building national compute capacity for artificial intelligence, OECD Digital Economy Papers, No 350, OECD Publishing, 2023, Paris.
[46] Edge Observatory for the Digital Decade, Edge Deployment Data report 1., 2023.

Together, the projects pursue the objective of building a high-performance cloud-edge infrastructure based on European values and ensuring European competitiveness. The aim is to create a multi-provider cloud-edge continuum.

The **IPCEI CIS** foresees important dissemination and spillover effects across the Union, beyond participating Member States and companies. Dedicated dissemination actions performed by the companies will play an important role[47].The **Cloud Infrastructure and Services Exploitation Resources Office (CISERO**), funded under the Digital Europe Programme, may provide, if and where necessary, assistance to the IPCEI_CIS participating companies in their primary efforts in delivering their dissemination and spill-overs actions.

Guiding future actions, the **Competitiveness Compass** highlights the importance of compute, cloud, and data infrastructures in strengthening Europe's AI capabilities.

An **EU Cloud and AI Development Act** will focus on equipping Europe with secure, modern, and sustainable infrastructure to scale up Europe's computational capacity. By mobilising public and private initiatives, it will support the **deployment of infrastructure for training very large AI models**, **enabling key AI ecosystems** throughout the EU, in addition to addressing **capacity gaps and supporting investments in sustainable and sovereign cloud, edge, AI and telecom networks infrastructure**. The Act will also set focus on **cutting red** tape to stimulate investment, accelerating permitting procedures, and improve access to land, finance and energy.

Complementary to these developments, several Member States in the context of the Joint European Forum for IPCEI (JEF-IPCEI) in November 2024 decided to enter the **design phase of two new potential IPCEIs**. The first one on innovative AI Services (IPCEI-AI), with a focus on R&D&I and first industrial deployment of AI compute technologies and services; and a second one on deploying computing infrastructure (IPCEI-ECI) across the EU territory.

The need to step up investments

Access to large-scale computing power is essential for advancing technological capabilities in AI in general, and particularly in the development of large languages models (LLMs). AI is a key driver of increasing demand for compute capacity, but not the only one, as general cloud workloads are also on the rise.

In February 2025, Commission President Ursula von der Leyen launched InvestAI, a major initiative aimed at mobilising EUR 200 billion for AI investments, including the establishment of a new EUR 20 billion European fund dedicated to AI gigafactories. These gigafactories will be equipped with at least 100 000 next-generation AI chips, four times the capacity of current AI factories under deployment. While the gigafactories funded through InvestAI will represent the world's largest public-private partnership in high performance for the development of reliable AI, additional AI compute resources

[47] For example they will (i) beyond their usual open-source software practices and business models, grant permissive, non-restrictive open-source software licenses to any interested party and actively engage with and contribute to the development of open-source communities; (ii) provide access to interested parties to at least 20% of the capacity of the edge nodes and laboratories employed in their projects; (iii) expand the developed technologies to additional economy sectors; (iv) perform targeted trainings, produce self-standing technical materials, engage in conferences, publications, partnerships with universities and research organisations; and (v) license intellectual property rights at fair, reasonable, and non-discriminatory terms.

in traditional cloud and edge data centres will be necessary to meet the broader AI compute demands of business and society across the EU. In 2023, average construction costs for a data centre in the EU reached EUR 8.4 million per MW[48] and cloud providers point at investment needs of at least EUR 1 billion for 200-300 MW of installed capacity. The future Cloud and AI Development Act will contain measures to boost the deployment of sustainable data centres in the EU, including through faster permit procedures. Currently, the average time to obtain a permit to build a greenfield data centre and the related environmental authorisations lies upwards of 48 months. The Cloud and AI Development Act will explore way of paving the way towards simplifying the deployment of data centres in the EU that are highly sustainable and innovative.

1.1.3.4 Quantum technologies and High-Performance computing

Progress towards the Digital Decade target

Target: Secure, resilient, performant and sustainable digital infrastructures where the Union has, by 2025, its first computer with quantum acceleration, paving the way for the Union to be at the cutting edge of quantum capabilities by 2030.

Source: Key Performance Indicators for the monitoring of quantum technologies in Europe (prepared by the Strategic Advisory Board of the Quantum Flagship)[49].

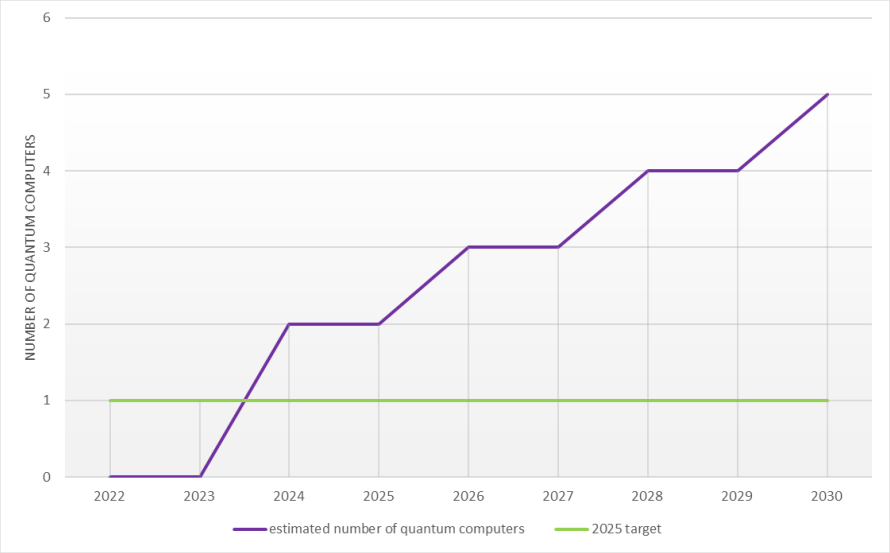
Available data points: from 2022 to 2024.

2024 data point: 2.

The starting value for this KPI is 0 in 2022 and it reached and overtook the target in 2024 as the first two quantum simulators were deployed in France and Germany[50], see trajectory in the figure below. It is expected that six additional quantum computers will be deployed until the end of 2025 as several procurements are currently ongoing. Due to the specificity of this target, no baseline trajectory is established.

[48] Savills Data Centre, European Data Centres Navigating the new data-centric frontiers, 2024.
[49] Quantum Flagship, Key performance indicators, 2024.
[50] Key Performance Indicators for Quantum Technologies in Europe, Strategic Advisory Board of the European Quantum Flagship, 2025.

Figure 14: Number of quantum computers in the EU. Trajectory towards 2030



Note: The quantum computing trajectory is based solely on an assessment by experts (same as in the '2024 Communication on EU-level trajectories').

The EU's leading role in quantum technologies

Quantum technologies are poised to revolutionise multiple industries, driving innovation in healthcare, transportation, energy, defence, chemicals, and pharmaceuticals. Recognising their strategic importance, the EU launched the **Quantum Technology Flagship** in 2018, committing EUR 1 billion over a decade to reinforce Europe's leadership in quantum research and transform breakthroughs into impactful applications. Thanks to additional national programmes, total funding has grown to EUR 7 billion.

Quantum remains a global priority, with frequent technological breakthroughs and increasing geopolitical focus and regions taking measures to secure their interests in this strategic field. In 2024, for instance, the Commission and Member States embarked on a joint risk assessment for quantum in line with the EU's economic security strategy[51], while the United States started to impose export controls on quantum computing, reshaping global supply chains and potentially limiting EU companies' access to key technologies.

In global terms, the **EU remains a leading source of public funding for research and innovation in quantum**, and European efforts were given renewed impetus by the signature of the Quantum Declaration by 26 Member States confirming the strategic importance of quantum technologies and committing to collaborating on the development of a world-class quantum technology ecosystem across Europe[52]. Still**, Europe lagged behind other regions in the availability of private finance needed for the most promising EU start-ups in quantum to scale up**, an issue highlighted in the report on 'The Future of European Competitiveness' where it is reported that 'for quantum

[51] In line with Commission Recommendation of 03 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States, (C(2023) 6689 final).
[52] European Commission, European declaration on quantum technologies, 2025.

computing, EU companies attract only 5% of global private funding compared with a 50% share attracted by US companies'[53].

According to another independent report by Olivier Ezratty[54], several US quantum firms attracted private VC funding in hundreds of millions of dollars whereas most EU start-ups operate with under EUR 20 million. This limited private fund hinders the scale-up capacity and contributes to brain drain and IP migration. Moreover, it creates dependence on non-European capital and platforms, putting Europe's quantum sovereignty at risk, especially for hardware and full-stack quantum solutions.

The announcement of the European Innovation Council's new STEP Scale up scheme[55], offering up to EUR 900 million of deep tech scale-up funding for EU start-ups in strategic sectors, particularly in quantum technologies, will help to partially remedy this. The objective of this new scheme is to support start-ups, SMEs and small mid-caps through investments between 10 and 30 million.

Through its existing programmes, EIC Pathfinder, EIC Transition and EIC Accelerator, the **European Investment Council already invested over 200 million EUR in all the fields of quantum technologies:** sensing, communication and computing. These investments will continue in order to ensure accelerated growth, scaling, and international competitiveness for European quantum start-ups.

The Commission, together with the EIC, is set to put in place several initiatives targeted at providing dedicated financial resources and for quantum start-ups and SMEs to support their growth, product development, and market entry. These initiatives are expected to offer start-ups expert mentoring in quantum technology commercialisation, intellectual property management, quantum market analysis, and access to leading quantum testbed infrastructure provided by European Quantum Excellence Centres and national quantum hubs.

As quantum companies move through the EIC programmes, the Commission will establish structured guidance and dedicated support for quantum companies transitioning from EIC Pathfinder and Transition programmes into the Accelerator, ensuring coherent support throughout their technology and business maturation processes. In parallel, the Commission is supporting the development of Quantum Pilot Lines, which will provide the first industrial manufacturing capabilities for key quantum components in Europe. These pilot lines aim to bridge the gap between research and market deployment, fostering the emergence of a competitive quantum industry.

The Quantum Strategy and Quantum Act to be published in 2025 and 2026 respectively will outline additional measures for EU's ambitious plans to establish itself as the global leader in quantum technologies by 2030 and beyond.

The EuroHPC JU & the 'AI factories' Initiative

On supercomputing, the EU's commitment to establishing a full competitive supercomputing infrastructure is embodied in the HPC JU, launched in 2018 with a budget of nearly EUR 7 billion for 2021-2027, co-funded by the EU, Participating States, and private actors. Over the past five years, the EuroHPC has contributed to the acquisition of eight supercomputers, including notable examples

[53]Draghi, M., The future of European competitiveness, 2024.
[54] Opinions Libres, Understanding quantum technologies 2024, 2025.
[55] European Innovation Council, STEP scale up European Innovation Council, STEP scale up. Available at: https://eic.ec.europa.eu/eic-funding-opportunities/step-scale_en

such as LUMI (ranked #8 globally), Leonardo (#9), and MareNostrum 5 (#11)[56], which collectively multiply Europe's computational capabilities, and the first European system to reach the exascale[57] frontier (JUPITER). A second exascale supercomputer (Alice Recoque) is to be installed within the next year. With the launch of the AI Factories, the EU will equip itself with at least six additional supercomputers in 2025 -2026 to match the EU's ambition of becoming the AI Continent. These efforts have propelled the development of a world-leading, secure, and interconnected supercomputing ecosystem, broadening the use of high-performance computing (HPC) and cultivating essential skills for European science and industry.

European High-Performance Computing Joint Undertaking (EuroHPC) is *de facto* contributing to the Digital Decade's objective to have a first European computer with quantum acceleration by 2025, paving the way for cutting edge quantum capabilities in the EU by 2030. In this respect, EuroHPC has already selected **eight sites across the EU to host the first EU quantum computers** in Czechia, Germany, Spain, France, Italy, Poland, Luxembourg and the Netherlands.

On 9 July 2024, an amendment to the regulation on the European High Performance Computing Joint Undertaking (EuroHPC JU) – the 'AI Factories Act' – entered into force, with enlarged objectives for the EuroHPC including the development and operation of AI Factories. The AI Factories consist of deploying and operating AI dedicated supercomputers connected to large data centres, enhancing the performance of these supercomputers by regularly upgrading their AI capabilities. AI Factories will also provide AI-dedicated supercomputing services in support of the AI start-up and research ecosystem for the large-scale training and development of general purpose, trustworthy and ethical AI models and systems, and of AI user communities for the development, validation and running of emerging AI applications, in particular in the areas of health and care, climate change, robotics, and connected and automated driving. AI Factories will also foster talent development with advanced education, training, skilling and reskilling activities for relevant AI stakeholders.

The AI Factories will create synergies at EU level and will cooperate with, and federate other relevant EU AI initiatives, such as the Artificial Intelligence On-Demand platform, the AI Testing and Experimentation Facilities, the EuroHPC Competence Centres, the EuroHPC Centres of Excellence, and any other emerging European AI initiatives. These changes will enable the Joint Undertaking to offer tailored computing power and services to nurture large-scale AI training and development and uptake in the EU.

The Commission has already announced the initial 13 AI Factories' hosting entities, bringing together 17 Member States and two associated EuroHPC participating states. This initiative will be complemented with a call to establish AI Factory Antennas in additional participating states, providing access to established AI Factories' supercomputers. The existing support for AI Factories of around EUR 2 billion, co-financed by the EU and the Member States, is already the largest public investment in AI infrastructure in the world.

Conclusion and way forward

Over recent years, EU and Member States have undertaken significant efforts to advance the work towards the achievement of the KPI for quantum technologies, as defined in the Digital Decade Policy

[56] Top500 list, November, 2024.
[57] Systems capable of executing more than one trillion calculations per second.

Programme ('*Quantum computing measured as the number of operational quantum computers or quantum simulators, inc. as accelerators of HPC supercomputers, deployed and accessible to the user communities*'). Thanks to the continued commitment and substantive investment of resources both at EU and Member States level, the target of operationalising one such system by 2025 has been achieved ahead of schedule, with the deployment of two quantum simulators in France and Germany under the HPC-QS project already in 2024[58]. Additional systems are currently under deployment and are expected to become available by the end of 2025.

At the same time, looking ahead to 2025, the EU's initiatives on AI infrastructure demonstrate a strong foundation for establishing Europe as the leading AI continent.

Funding of AI Gigafactories with a mix of grants and equity will serve as one of the pilot cases for strategic technologies announced in the Competitiveness Compass[59].

In view of the recent US new export controls placing restrictions on advanced AI chips[60], the development of sovereign European technologies (e.g. RISC-V based accelerators) are taking additional relevance, to ensure the viability of these large-scale AI training facilities.

1.1.4 The digital Euro – contributing to a resilient payments ecosystem

The way that citizens and businesses use money is rapidly evolving. While the EU ensures the availability and acceptance of cash, its use is steadily declining. Between 2019 and 2024, the share of cash payments in the euro area dropped from 72% to 52% of point-of-sale transactions. Digital payments are steady increasing in value terms, with cards accounting for 48% of online transactions in 2024, and **mobile payment wallets and mobile apps together accounting for 29% of transactions**[61].

This shift raises critical questions about the role of central bank money in preserving monetary stability and financial sovereignty. Traditionally, cash has served as a 'monetary anchor' that guarantees the role of public money in the economy. However, as digital transactions grow, central banks must ensure that public money remains accessible and relevant. Globally, 107 jurisdictions are actively exploring their own central bank digital currency (CBDC) initiatives, with 44 in the pilot stages[62].

Stablecoins – issued by private entities and pegged to *fiat* currencies – have experienced significant growth in recent years, particularly in market capitalisation. Currently, approximately 99% of the global stablecoin market capitalisation is denominated in US dollars, with the vast majority of digital asset transactions also conducted in US dollars[63]. In the future, non-euro denominated stablecoins could serve as a systemic tool for cross-border payments: this could risk weakening the role of the euro in European and international retail payment markets.

Today, the EU lacks a unified payment system, and while some countries have their own national payment systems, the EU as a whole relies heavily on international card schemes, representing over

---

[58] HPC QS, High performance computer – quantum simulator hybrid. Available at: https://www.hpcqs.eu/.
[59] European Commission, An EU compass to regain competitiveness and secure sustainable prosperity, 2025.
[60] Federal Register, Framework for artificial intelligence diffusion, 2025.
[61] European Central Bank, Study on the payment attitudes of consumers in the euro area (SPACE), December, 2024.
[62] Atlantic Council, Central Bank Digital Currency Tracker, 2025.
[63] DefiLlama, Defi Dashboard, 2025. Available at: https://defillama.com/

64% of all card-initiated transactions in the euro area[64]. This external dependence exposes the EU to geopolitical and cybersecurity risks.

The digital euro would be designed to strengthen the EU's sovereignty, economic security, and competitiveness by providing a public digital payment solution that complements private options. This would ensure a competitive and reliable alternative in an era where non-European payment solutions and foreign digital currencies are growing[65].

The legislative proposal establishing the digital euro and regulating its essential elements was adopted by the Commission in June 2023. The legislative process progressed in 2024, with the European Parliament and Council continuing negotiations within each of the institutions.

The final decision on issuing the digital euro, including its technical design choices, will be taken by the European Central Bank after the legislative process is concluded. The ECB's two-year preparation phase, running until Autumn 2025, includes defining a digital euro public scheme through the Rulebook Development Group, selecting providers for infrastructure development, and testing technical aspects such as offline functionality and the roll-out plan. National central banks within the Eurosystem have been actively involved in the ECB's preparation phase, contributing to technical development and stakeholder engagement.

The digital euro's successful implementation will depend on a wide variety of technical, legal and economic factors, including the role of the private sector. Developing a digital euro requires significant investment in infrastructure, cybersecurity, and user adoption. While the Eurosystem will bear its own costs, public funding alone will not suffice. Private investment and industry collaboration are essential to ensure a secure and efficient ecosystem. Large-scale adoption depends on seamless integration with existing point-of-sale terminals, mobile apps, and banking interfaces. Investment is required to ensure interoperability with existing private payment systems. Looking ahead, investment will be essential to develop robust digital payment systems capable of enhancing cybersecurity and ensuring seamless interoperability between public and private financial solutions[66].

A key innovation is the offline/proximity functionality, allowing small transactions without third-party validation, ensuring a higher level of privacy. Implementing this feature requires investment in hardware security, cryptographic protocols, and tamper-resistant storage. Depending on the design choices, secure offline wallets may include hardware-based solutions (e.g. secure elements in smartphones) or dedicated offline payment cards.

The digital euro will be widely accessible and inclusive. Offline use is relevant for areas of poor internet connectivity and for frictionless payments in situations such as high-speed trains or underground parking. Beyond being a fallback option, offline payments will support users' privacy preferences. Further, the digital euro supports financial and digital inclusion by allowing people without bank accounts to open digital euro accounts easily (e.g. at entities specifically designated by Member States, such as post offices) so that they can use basic services free of charge.

---

[64] Volume share of international card schemes in total electronically initiated card payments with cards issued in the euro area and transactions acquired worldwide for the first half of 2023. Based on data collected under Regulation (EU) No 1409/2013 of the European Central Bank on payments statistics (ECB/2013/43), as amended.

[65] Bellia, M., Di Girolamo, F. E., Nai Fovino, I., Petracco, M., Sportiello, L. and Vespe, M. (2023), Future of the euro: pay everywhere and whenever you want, Science for Policy Briefs, European Commission, Joint Research Centre, Ispra. JRC134382.

[66] Draghi, M. The Future of European Competitiveness—A Competitiveness Strategy for Europe, 2024.

Conditional payments – transactions automatically executed upon meeting predefined conditions set by users – will also require investment. Public-private partnerships will play a crucial role in ensuring that payment service providers can offer this feature to users.

The digital euro and the potential for simplification

The legislative proposal also foresees that when performing digital euro transactions and opening digital euro accounts, users can easily identify, authenticate, and authorise payments via the European Digital Identity Wallets. Furthermore, thanks to the interoperability and synergy between the digital euro and the European Digital Identity Wallets, users will be able to access various public and private services in the digital economy via a secure and privacy-by–design solution, with streamlined costs for the industry.

Overall, progress has been made in laying the groundwork for the digital euro, following the European Commission's legislative proposal in June 2023 and the ECB's ongoing preparation phase.

A well-structured digital euro should offer benefits for consumers, financial institutions, and businesses by reducing costs, increasing competition, and strengthening financial resilience.

1.2 Digitally transformed and competitive industries

Europe's competitiveness is affected by lower productivity compared to its global competitors, which can be tied to the insufficient diffusion of digital technologies, which impacts the ability to use tech to develop new services and business models[67].

1.2.1 Digitalisation of SMEs

Progress towards the Digital Decade target

Target: the digital transformation of businesses, with more than 90% of the EU's SMEs reaching at least a basic level of digital intensity[68].

Source: Eurostat – European Union survey on ICT usage and e-commerce in enterprises (code: ISOC_E_DII[69]). Since 2021, two different versions of this indicator are measured every second year: Digital Intensity Index (DII) version III measured in 2021 and 2023; DII version IV measured in 2022 and 2024. DII version III is expected to be available for both 2025 and 2026.

Available data points: from 2015 to 2024. Only DII versions 3 and 4 are currently used, available since 2021. Break in series every year, except for DII version III, years 2021 and 2023 are comparable, and for DII version IV, years 2022 and 2024 are comparable.

[67] Europe's choice, Political Guidelines for the next European Commission 2024–2029, p. 9. European Commission, Europe's choice, Political Guidelines for the next European Commission 2024–2029, 2024. p. 9.

[68] As defined in Commission Implementing Regulation (EU) 2021/1190 of 15 July 2021 laying down the technical specifications of data requirements for the topic 'ICT usage and e-commerce' for the reference year 2022, and subsequent implementing regulations pursuant to Regulation (EU) 2019/2152 of the European Parliament and of the Council (Text with EEA relevance), in particular Article 7(1) and Article 17(6).

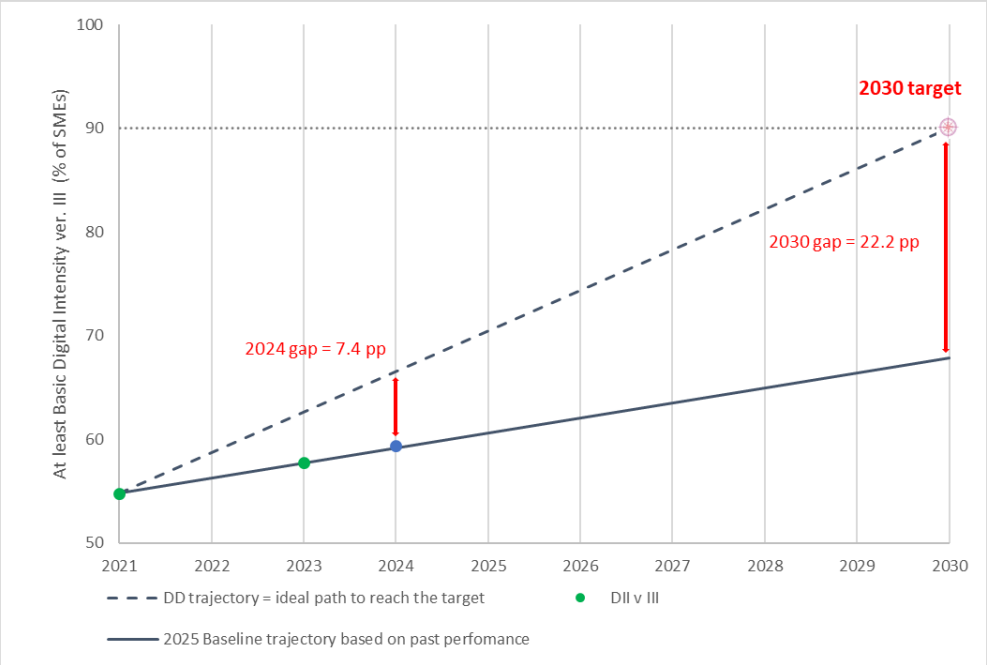
[69] The KPI is computed as the complement to 100 of the percentage of SMEs with a very low digital intensity index (sub-category E_DI4_VLO).

2024 data value (DII version IV): 72.9% (annual growth used to estimate DII version III baseline trajectory = 2.8%).

The percentage of SMEs with at least a basic level of digital intensity (version IV) rose by 3.9 percentage points in two years, from 69.0% in 2022 to 72.9% in 2024. This reflects a modest year-on-year increase of 2.8%.

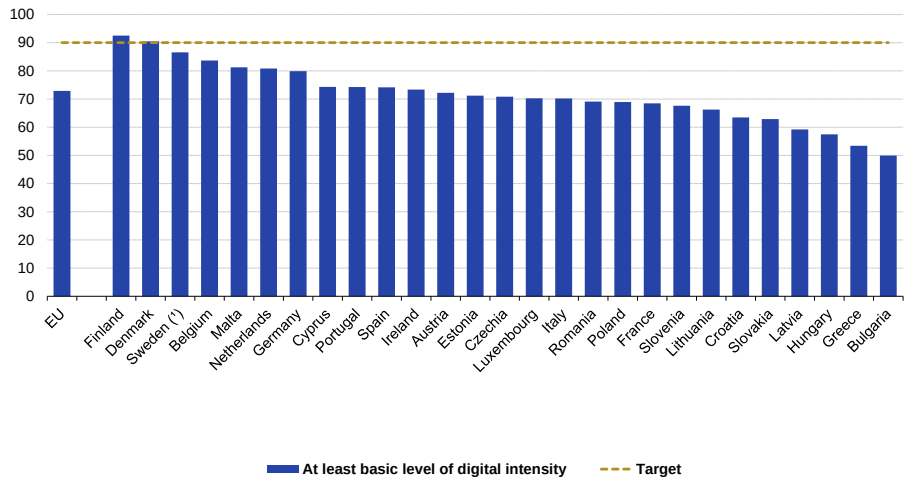
According to the forecast along the baseline trajectory based on DII version III, only 75% of the target is expected to be achieved by 2030, with an estimated 67.9% of SMEs having at least a basic level of digital intensity by then. In 2024, the value reached by this KPI stood at about 89% of the ideal value along the digital decade trajectory (59.2% instead of 66.5%). The target is expected to be reached not earlier than 2045 if no further actions are taken.

Figure 15: Digital Intensity Index version III. Historical comparable data, estimated 2024 data point, Digital Decade (DD) trajectory and revised baseline trajectory towards 2030



Even though EU Member States are making a considerable effort to advance business digitalisation, progress remains uneven across Member States and sectors. While some Member States have already achieved the 90% target (Finland and Denmark), others are still catching up, with some countries trailing well below the EU average.

Figure 16: Enterprises with at least a basic level of digital intensity, 2024 (% of SMEs)

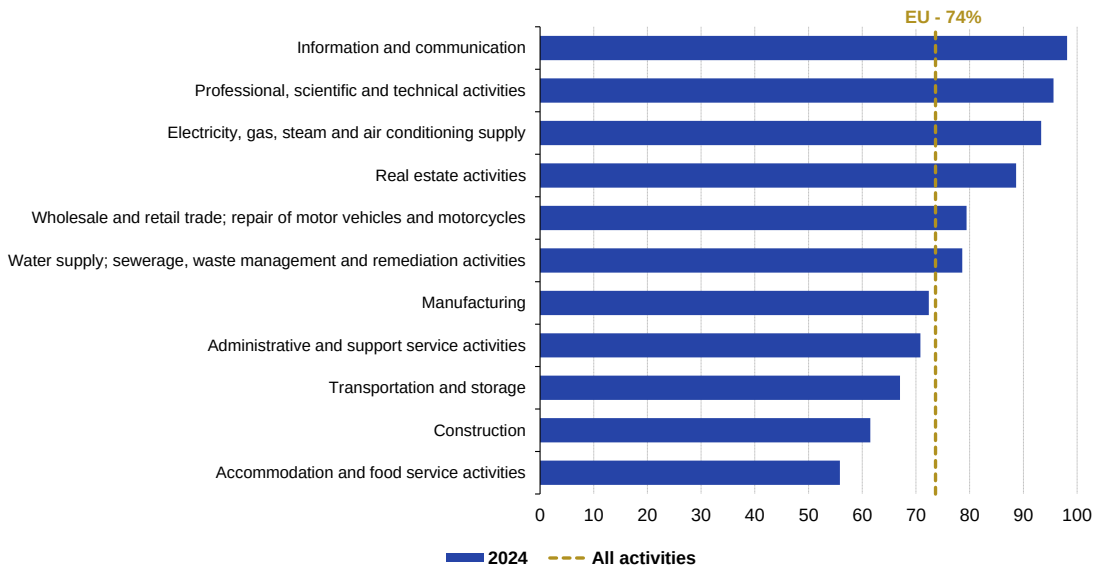


(*) Break in the time series

Source: Eurostat (online data code: isoc_eb_diin2)

Similar variations can also be seen across the different sectors, with the level of digitalisation varying significantly from sectors like ICT to more traditional ones like construction or accommodation and food service activities.

Figure 17: Enterprises with at least a basic level of digital intensity (DII version IV), by economic activity, EU, 2024 (% of enterprises)



Source: Eurostat (online data code: isoc_eb_diin2)

SMEs face several challenges in digitalising their operations, including a lack of awareness about the resulting benefits, limited access to finance, and gaps in digital skills. To address these challenges, various initiatives have been implemented across the region. Common strategies to support SME digitalisation include knowledge-building activities, funding initiatives, and ecosystem collaboration.

Knowledge-building efforts help SMEs understand digital technologies' benefits, often through events, workshops, and training programs that focus on upskilling employees. Funding initiatives, such as grants and tax incentives, are also widely offered to reduce the financial burden of digital transformation. Moreover, ecosystem collaboration, particularly through partnerships with research institutions and other stakeholders, enhances SMEs' access to information and expertise[70].

A pivotal component of these efforts is the **European Digital Innovation Hubs (EDIHs) Network. Launched in 2023** and covering nearly 90% of EU regions, it supports SMEs and public sector organisations in adopting advanced digital technologies like AI and big data. EDIHs provide significant services, including networking, skills development, investment support, and opportunities to test digital solutions before investing.

The EDIH Network has organised numerous events and conducted thousands of digital maturity assessments to help firms identify strengths and areas for improvement. On average, firms engaging with EDIHs show a moderate level of digital maturity, and many demonstrate progress over time. Most SMEs that undergo follow-up assessments report increased digital maturity, highlighting the essential role of these initiatives in fostering digital transformation across Europe.

Insights on the path to digitalisation from the activities of the EDIHs

By employing the **Digital Maturity Assessment Tool (DMAT)**, EDIHs assess the digital maturity of SMEs across six key dimensions: Digital Business Strategy, Digital Readiness, Human-Centric Digitalisation, Data Management, AI & Automation, and Green Digitalisation. The results provide insights into the diverse digitalisation journeys undertaken by SMEs.

Recent findings reveal that SMEs engaging with EDIHs average a digital maturity score of 40 out of 100, indicating moderate digitalisation. Notably, AI & Automation scores are particularly low, at just 19, suggesting early-stage adoption of these advanced technologies. On the other hand, Data Management contribute more positively to overall scores.

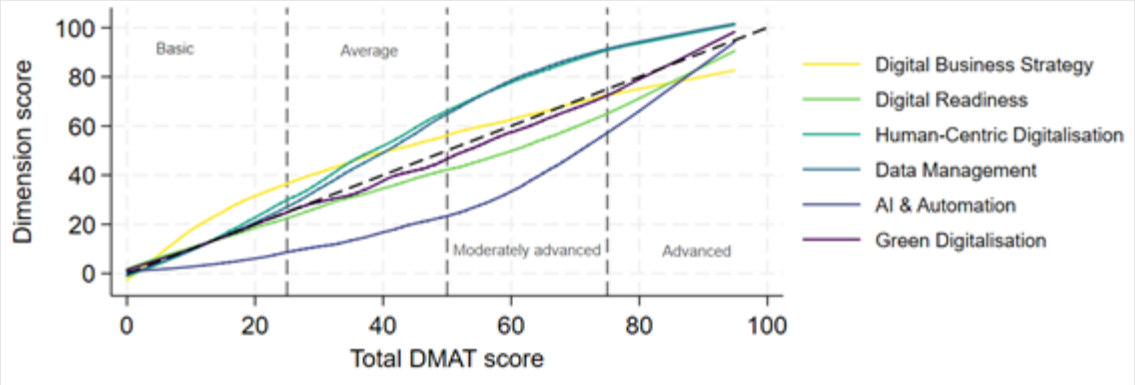
The distribution of DMAT scores varies widely among participating firms, with the Financial and Insurance sector and the Information and Communication sector leading in digital maturity. In contrast, the Agriculture, Forestry, and Fishing sector scores lowest on average.

Progression in digital maturity is evident; firms generally need to reach moderate digital maturity before significantly leveraging AI and Automation. Advanced digital developments depend on robust data management, security, and employee engagement in digital strategies (see chart below). Furthermore, follow-up assessments show that, on average, firms increase their overall DMAT scores by 7 points around one year later, with 90% demonstrating improved digital maturity[71].

Average DMAT dimension scores at different levels of digital maturity

[70] Study on Digitalisation of Business in the EU Member States: Initiatives, Impacts and Contribution to the Digital Decade 2023-26, 2025.

[71] European Commission: Joint Research Centre, Nepelski, D. and Stake, J., The EDIH SME DMAT 2.0*: Revision of the EDIH Digital Maturity Assessment Framework for SMEs*, Publications Office of the European Union, Luxembourg, 2024, JRC141446.



Note: The dimension score is estimated using locally weighted regression analysis.
Source: JRC elaboration

Member States' efforts

Best Practice Accelerator: technology take-up

To help EU Member States overcome challenges in the take-up of advanced technologies, a **Technology Take-up Cluster** was launched in August 2024 under the leadership of Belgium. As a key component of the Best Practice Accelerator (BPA) within the governance of the Digital Decade Policy Programme, its primary goal is to share and record high-level initiatives at government level that can be replicated in Member States to promote tech take-up. There have been two workshops focusing on AI uptake and data and interoperability, with presentations from Belgium and Finland. In addition, eight best practices have been submitted to the Best Practice Repository, available to all Member States. A short description is provided below:

Belgium has contributed two practices. The first, 'Start AI', connects organisations with AI experts to help identify and harness AI potential, with 98% of participating companies recommending the initiative to others. The second, Althumi, is dedicated to streamlining processes in smart societies by empowering citizens to control their personal data.

Denmark has introduced an SME grant scheme, which aims to clarify the digitalisation potential for small and medium enterprises, connects them with suitable solution providers, and offers assistance throughout the implementation process.

Finland has showcased 'RELEX Solutions' as a testament to successful start-up innovation and support. This solution tackles inefficient supply chain and retail operations by providing tools for optimising demand forecasting, inventory management, and retail planning. As a result, businesses can reduce waste, improve product availability, and enhance profitability.

Hungary has submitted 'KKV Digital', a self-assessment tool designed to measure digital intensity in SMEs that stands out by assessing businesses using 23 criteria.

Germany has presented two notable practices: the 'AI Opportunity Market' (MaKi) and the federal IPv6 Programme. MaKi aims to create a comprehensive platform for AI systems in federal administration, eventually extending to federal states and municipalities. The federal IPv6 Programme assists in the implementation of the IPv6 internet protocol across 142 individual migration projects with federal authorities and organisations.

Lastly, the **Netherlands** has devised a National Technology Strategy that highlights the ten

technologies (including AI, data science, semiconductors, quantum technologies, and cyber technologies) that will be given priority when it comes to innovation subsidies and strategic efforts.

1.2.2 Take-up of advanced digital technologies

In order to build and uphold a robust and sovereign Europe, the take-up of advanced technologies is of the utmost importance. Other than increasing productivity by allowing for automation, carrying out AI analysis and reducing costs for European enterprises, the use of pioneering technology also drives innovation, attracts talent and boosts private investment. Additionally, an increased use of advanced technologies also answers the call for securing European sovereignty. By reducing European reliance on external factors from outside the internal market, we will ensure strategic independence in a geopolitical landscape which is changing rapidly around us. As private and public actors within the EU become more digitalised, trust in public institutions will be strengthened, and we will be less fragile when met by disinformation or other disruptions spread by malign entities.

Progress towards the Digital Decade target

Target: The digital transformation of businesses, where at least 75% of EU enterprises have taken up one or more of the following, depending on their business operations: (i) cloud computing services; (ii) data analytics (as of 2024); (iii) artificial intelligence.

Source: Eurostat – European Union survey on ICT usage and e-commerce in enterprises.

Available data points: Cloud: 2014, 2016, 2018, 2020, 2021 and 2023 (break in series in 2021); Data analytics (big data before 2023): 2016, 2018, 2020 and 2023 (break in series in 2023); AI: 2021, 2023 and 2024.

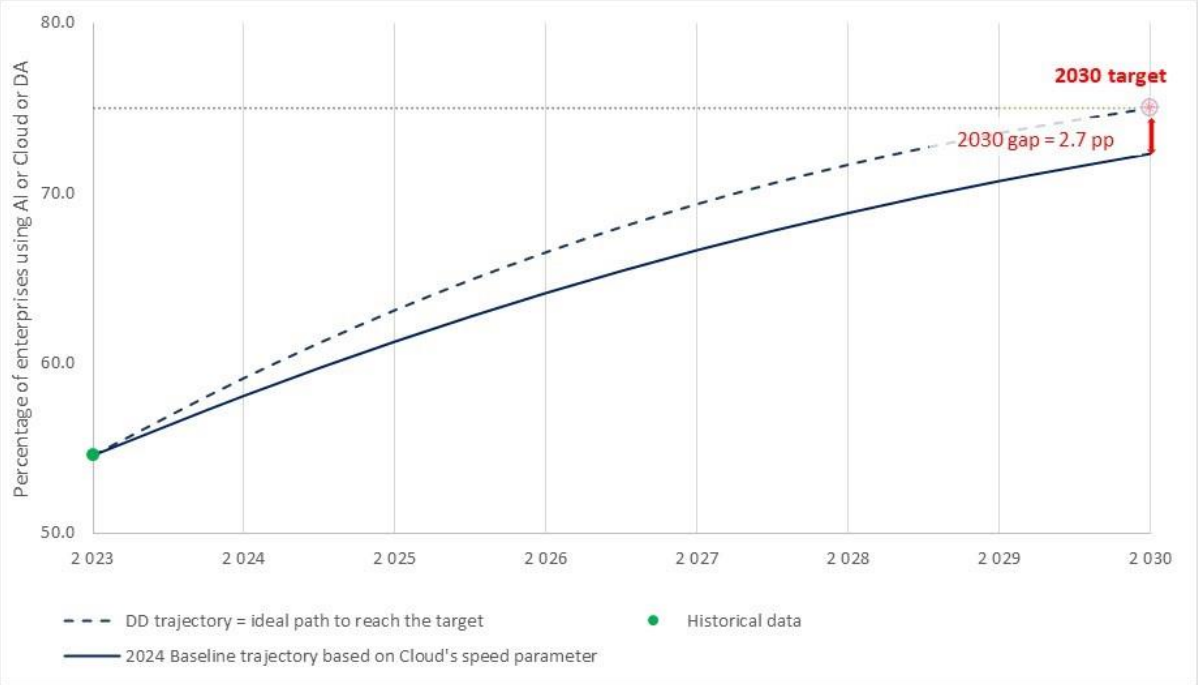
2024 data values: AI = 13.5%

(No 2024 data for Cloud, Data Analytics and 'AI or Cloud or Data analytics')

The percentage of enterprises using artificial intelligence or cloud computing services or data analytics stood at 54.7% in 2023. No other data point is available, therefore the speed of diffusion of the baseline trajectory is estimated on the basis of the cloud KPI. The timing of diffusion is instead computed based on the 2023 observed value.

According to the forecast along the baseline trajectory, **96% of the target is expected to be achieved by 2030,** with 72.3% of enterprises expected to use at least one of the three key technologies by then. The target is expected to be reached in **2032** if no further actions are taken.

Figure 18: 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)



Among SMEs, the uptake was slightly lower at 53.74%, whereas a significantly higher proportion of large enterprises – 86.71% – adopted these technologies. This reflects a percentage point difference of 32.97 between SMEs and large enterprises, indicating that while usage was widespread across all enterprise sizes, large enterprises tended to engage with these technologies at a markedly higher rate than SMEs.

The box below provides insights on the uptake of several advanced technologies across industrial ecosystems, showing a general upward trend.

Adoption of advanced technologies by industrial ecosystems

When analysing the progress made in the adoption of advanced technologies by industrial ecosystems, it was clear that there was a leap forward for several advanced digital technologies in 2023. Results show that cloud technologies have significantly progressed in terms of adoption across all ecosystems, closely followed by AI, which has recently seen significant growth in the adoption rate in some ecosystems. The adoption rate of connected devices (internet of things) also increased notably, although it is more specific to certain ecosystems such as electronics, aerospace, defence and health.

The industrial ecosystems that made the most overall progress since last year in adopting digital technologies include aerospace and defence, electronics and the cultural and creative industries, all of which saw an increase of over 10 percentage points. The figure below shows the progress in the adoption rate of digital technologies by industrial ecosystem.

	Artificial Intelligence	IoT	Cloud	Robotics	Big data	AVR	Blockchain	Edge computing
Aerospace & Defence	30.82%	21.38%	14.04%	6.72%	9.83%	8.06%	2.93%	3.84%
Agri-Food	11.03%	13.80%	10.57%	8.69%	-4.34%	-4.02%	2.47%	2.78%
Construction	28.27%	12.97%	24.79%	1.36%	5.05%	6.39%	0.35%	6.62%
Cultural & creative industry	6.17%	10.77%	10.75%	3.96%	0.68%	3.09%	0.15%	-2.39%
Electronics	31.43%	34.72%	26.89%	4.98%	11.43%	-0.06%	0.59%	10.53%
Energy intensive industry	13.06%	15.72%	8.09%	9.32%	2.24%	-2.29%	2.84%	-2.54%
Health	20.68%	10.85%	22.13%	1.45%	3.45%	-5.07%	4.79%	8.42%
Mobility Transport & Automotive	9.06%	24.79%	17.83%	6.85%	8.28%	-5.05%	1.79%	-0.79%
Retail	10.10%	6.30%	11.39%	4.21%	1.19%	-1.98%	-0.53%	4.29%
Proximity, Social economy & Civil Security	11.71%	0.04%	26.60%	3.10%	2.37%	-0.97%	0.00%	1.87%
Textile	17.74%	6.79%	0.42%	0.41%	0.12%	-3.05%	3.16%	5.94%
Tourism	14.94%	9.86%	12.46%	0.94%	0.00%	4.06%	4.22%	4.37%

The level of private-sector investment in digital technologies is relatively low when compared with global competitors. Robotics is the technology in which multiple industrial ecosystems (10 out of 12) invest over 5% of their annual turnover. The annual investment for SMEs in cloud computing is estimated at EUR 136.56 billion in total, making cloud computing the technology with the highest overall investment of all advanced digital technologies analysed in the European Monitor of Industrial Ecosystems project. When zooming in on individual industrial ecosystems, business investment in digital technologies may well exceed 5% of turnover. For instance, the electronics industrial ecosystem stands out for the high level of investment in cloud computing (23.19%), edge computing (22.73%), robotics (19.05%), IoT (12.28%) and big data (5.88%).

Source: EMI enterprise survey 2024

1.2.2.1 Take-up of cloud services

Cloud computing constitutes a foundation for innovation and growth. Access to cloud computing is the gateway for accessing processing power, storage, and software. Through the cloud, users can access these features on demand and have flexibility in adjusting the capacity purchased to their needs without upfront infrastructure investments. Cloud computing is thus a driver for innovation and competitiveness in today's digital economy. It is also the gateway to the computing capacity needed for AI, primarily for fine-tuning and inference.

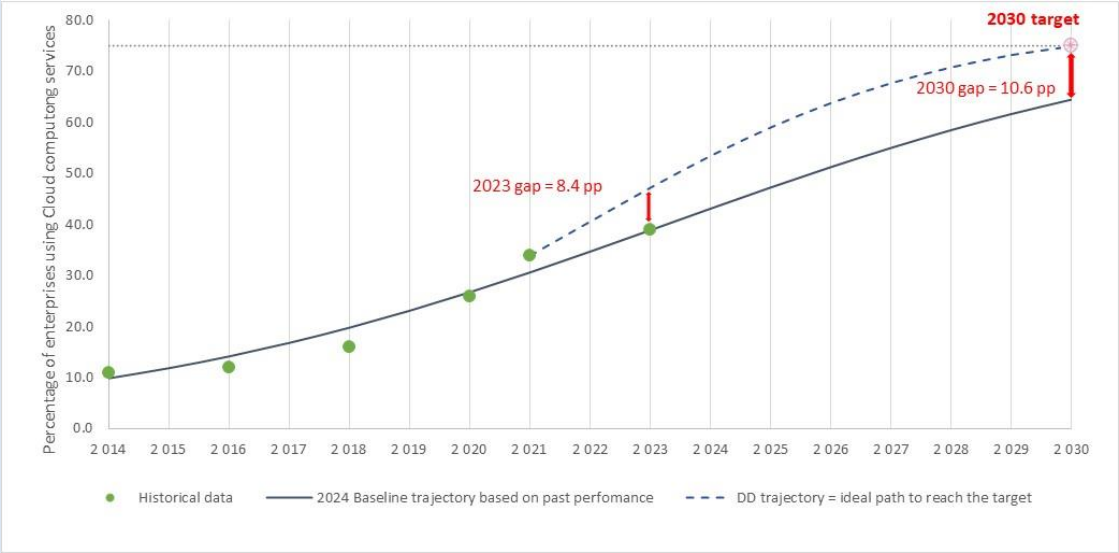
Progress towards the Digital Decade target

The percentage of enterprises using sophisticated or intermediate cloud computing services rose by 5 percentage points, from 34.0% in 2021 to 38.97% in 2023. This represents a year-on-year increase of 7.1%.

According to the forecast along the baseline trajectory, approximately 86% of the target is expected to be achieved by 2030, with 64.4% of enterprises expected to adopt sophisticated or intermediate cloud services by then. In 2023, the gap stood at about 82% of the ideal value along the digital

decade trajectory (38.9% instead of 47.3%). The target is expected to be reached not earlier than 2036 if no further actions are taken.

Figure 19: Percentage of enterprises using cloud computing services in the EU. Historical data, Digital Decade (DD) trajectory and revised baseline trajectory towards 2030[72]



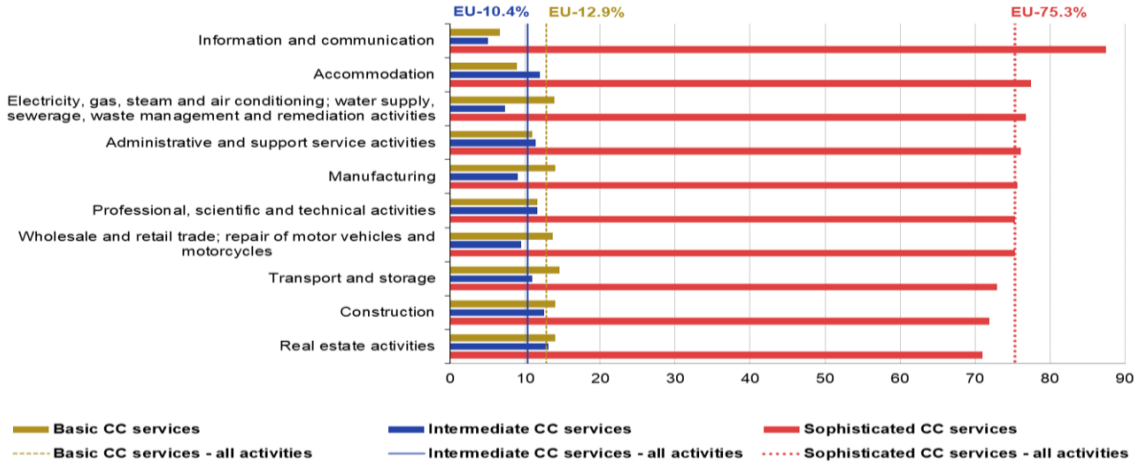
A **significant difference existed, however, in the degree of uptake among SMEs and large enterprises**. While nearly 2 out of 5 (38.04%) SMEs adopted cloud services, over 2 out of 3 (69.72%) large enterprises used these services. This indicates a 31.68 percentage point difference in uptake between SMEs and large enterprises at EU level.

Significant **differences** can also be seen **across Member States**, with the uptake rate ranging from 72.99% in Finland to below 20% in Greece, Bulgaria and Romania.

More detailed data show that enterprises are gradually moving towards higher levels of sophistication in terms of the types of services purchased, especially in some sectors.

[72]Eurostat's indicator 'Enterprises purchasing at least one of the following cloud computing (CC) services: hosting of the enterprise's database, accounting software applications, customer relationship management software, computing power' (code E_CC_GE_ME) is used for the period 2014-2020. A break in series occurred in 2021 when the indicator 'Enterprises buying sophisticated or intermediate CC Services' was used. This indicator includes different CC services: Accounting software (CC_PFACC); ERP software (CC_PERP); CRM software (CC_PCRM); Security software (CC_PSEC); Database hosting (CC_PDB) and Hosting environment for application development (CC_PDEV).

Figure 20: Level of sophistication of purchased cloud computing services by economic activity, EU, 2023 (% of enterprises buying cloud services)



Source: Eurostat (online data code: isoc_cicce_usen2)

Although the number of EU enterprises using cloud services is on the rise, the main providers of cloud computing services are US companies. Despite the continued expansion of EU cloud providers, US providers accounted for 72% of the market for infrastructure as a service (IaaS), platforms as a service (PaaS), and hosted private cloud in 2022. This trend is expected to persist, with US providers projected to drive 65% of data centre demand in Europe by 2028[73], reinforcing concerns about the EU's reliance on foreign cloud and AI computing infrastructure and the possible negative repercussions on sovereignty and operational autonomy.

Finally, it should also be considered that, for many businesses, the cloud is the gateway towards AI and adopting cloud services is a necessary first step that paves the way for their adoption of AI services.

2024 was marked by EU cloud providers advancing their compliance efforts. The Data Act entered into force in January 2024 and will enter into application on 12 September 2025. By enabling free, fast and fluid switching, the Data Act is designed to boost competition in the EU cloud market. The Data Act hinders lock-in practices and ensures that cloud service providers compete on performance and price, thereby opening up the market for cloud innovation and for providers to differentiate themselves from their competitors.

The higher level of competition and improved trust in cloud services is expected to have a positive effect on cloud uptake by EU enterprises. The Commission has launched a study to monitor whether the reduction of switching and egress charges is indeed producing effects in the EU cloud market, and another study to build the common EU repository for the interoperability of data processing services. Moreover, the work of the expert group on B2B data sharing and cloud computing will, over the course of 2025, feed into a Commission recommendation on standard contractual clauses for data processing services. These will serve as a voluntary compliance tool for the Data Act's provisions on cloud switching.

[73] McKinsey, The role of power in unlocking the European AI revolution, 2024.

Additionally, with AI driving up demand for data storage and processing, the announced Cloud and AI Development Act will ensure that the EU has sufficient cloud capacity and adequate data centre infrastructure to serve the needs of EU businesses and public administrations. The proposed Act must be viewed in the context of the Digital Decade and other complementing legislative frameworks, such as the Artificial Intelligence Act.

1.2.2.2 Take-up of data analytics

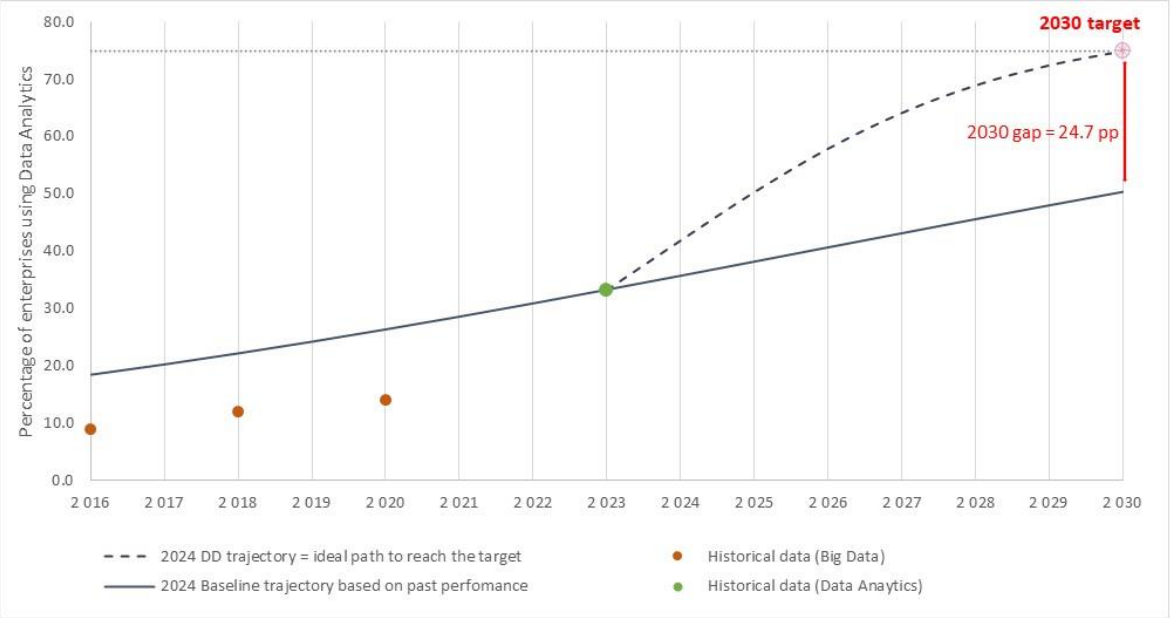
The data economy is based on the accessibility of high-quality data. If data is unavailable, new and innovative products and services might not be produced, thereby placing EU enterprises and public services at a disadvantage compared to their international counterparts. Consequently, it is necessary to break down technical, semantic and legal barriers to data sharing and use.

The European Strategy for Data, introduced by the Commission, sets forth a path to a true single market for data, where data will be available and flow freely within the internal market. The measures introduced, based on the strategy, will allow for further standardisation, interoperability, and the breakdown of legal barriers and will support the uptake of data analytics by – amongst others – EU enterprises.

Progress towards the Digital Decade target

The percentage of enterprises using data analytics stood at 33.3% in 2023. According to the forecast along the baseline trajectory, approximately 67% of the target is expected to be achieved by 2030, with 50.3% of enterprises expected to use data analytics by then. The target is expected to be reached not earlier than 2048 if no further actions are taken.

Figure 21: Share of enterprises using Data Analytics in the EU. Historical data, Digital Decade (DD) trajectory and baseline trajectory towards 2030



32.09% of SMEs adopted data analytics, while the percentage was significantly higher among large enterprises, with 71.81% using data analytics. This indicates a 39.72 percentage point difference in the use of data analytics between SMEs and large enterprises in the EU.

There are **differences among the Member States** as well: Hungary and Croatia are leading with rates above 50%, while Poland and Slovenia are lagging behind with rates below 20%.

The **2020 European Data Strategy** describes the vision of a European single market for data where data can flow freely across borders and sectors in full compliance with European rules and values. The strategy also laid down the foundations for common European data spaces in a set of vertical sectors of strategic importance for the European Union as a whole.

The strategy formed the basis for several legal acts (Data Act[74] and Data Governance Act[75]), the aim being to open up access to data. Both these acts work in tandem with existing rulesets, such as the GDPR[76] and the Open Data Directive (ODD)[77], and more recent rulesets, such as the European Health Data Spaces (EHDS)[78] and the AI Act[79].

Building on the 2020 European Data Strategy, the Commission is developing a European Data Union Strategy. The Data Union Strategy should aim to streamline existing data rules, potentially creating a simplified, clearer, and more harmonised legal framework for businesses and administrations to share data more seamlessly and at scale, while still upholding high privacy and security standards. Additionally, it may explore options to increase the availability of high-quality data, consider possible investments in data infrastructures, examine ways to use data to reduce the administrative burden, and address the external aspects of data flows.

1.2.2.3 Take-of up AI

Use of artificial intelligence technology is increasingly recognised as a key determinant of competitiveness not just in the high-tech sector, but across the whole economy.

Progress towards the Digital Decade target

The percentage of enterprises using AI rose by 5.4 percentage points, from 8.1% in 2023 to 13.5% in 2024. This represents a substantial year-on-year increase of 67%.

According to the forecast along the baseline trajectory, slightly less than half of the target is expected to be achieved by 2030, with 35.9% of enterprises expected to adopt AI by then. In 2024, the value reached by this KPI stood at about half the ideal value along the digital decade trajectory (13.5% instead of 28.4%). The target of 75% of enterprises using AI is expected to be reached in 2042 if no further actions are taken.

---

[74] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), PE/49/2023/REV/1, 2023.

[75] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), PE/85/2021/REV/1, 2022.

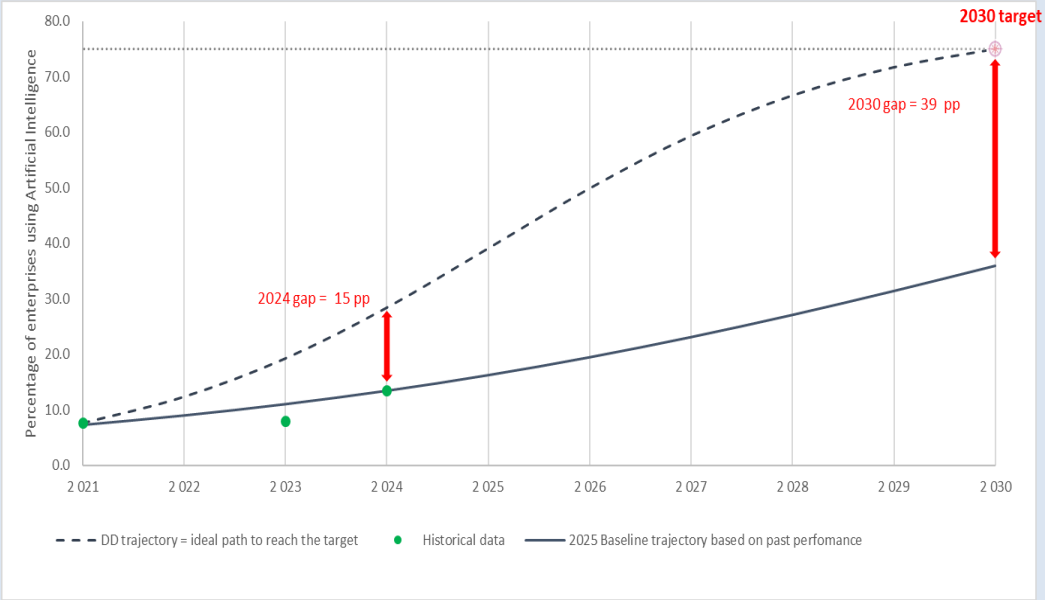
[76] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016.

[77] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), PE/28/2019/REV/1, 2019.

[78] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847, PE/76/2024/REV1, 2025.

[79] PE/24/2024/REV/1, 2024.

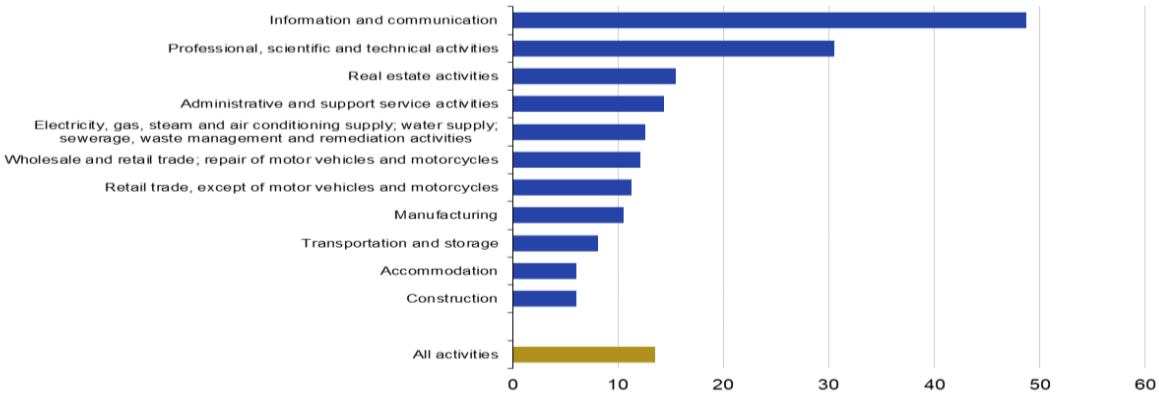
Figure 22: Percentage of enterprises using AI in the EU. Historical data, Digital Decade (DD) trajectory and revised baseline trajectory towards 2030



SMEs had an uptake rate of 12.64%, while large enterprises demonstrated a significantly higher usage rate of 41.17%. This reveals a 28.53 percentage point difference in the use of AI between SMEs and large enterprises in the EU. **It is particularly encouraging to note that growth among small enterprises shot up by no less than 71%, vastly outpacing the relative increase of 35% by large companies.** Thus, small companies are starting to catch up.

Two sectors are driving uptake: the information and communication sector and the professional, scientific and technical activities sector, whereas the construction and accommodation sectors are well below the average.

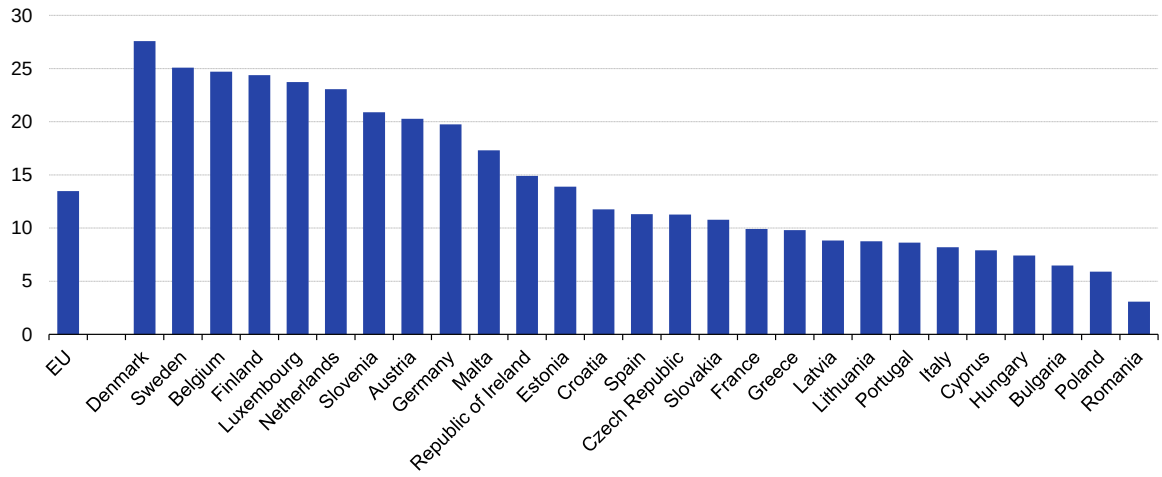
Figure 23: SMEs using AI technologies by economic activity, EU, 2024



Source: Eurostat (online data code: isco_eb_ain2)

At the same time, uptake differs greatly among Member States, from 27.6% in Denmark to about 3.1% in Romania. Nevertheless, growth is well distributed across EU Member States, with some countries which had previously very low AI uptake displaying the highest growth rates.

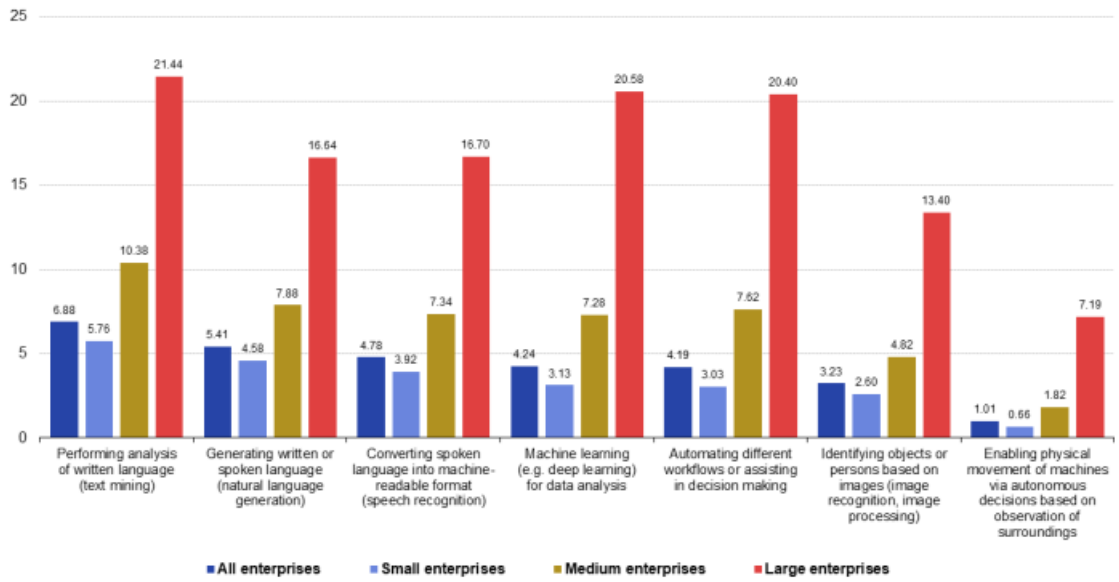
Figure 24: Enterprises using AI technologies by Member State, EU, 2024



Source: Eurostat (online data code: isco_eb_ai)

EU enterprises utilised various AI technologies, with no single technology dominating. In 2024, 6.88% used AI for written language analysis (text mining), followed by 5.41% using natural language generation. Other technologies, such as speech recognition, machine learning for data analysis, workflow automation, and image recognition, were used by 3.23% to 4.78% of enterprises. Only 1.01% used AI for autonomous machine movement.

Figure 25: Enterprises using AI technologies by type of AI technology and size class, EU, 2024, % of enterprises



Source: Eurostat (online data code: isco_eb_ai)

Overall, current data on AI use in the EU shows that ubiquitous AI usage is still a long way off, but that progress is promising.

Following the launch of ChatGPT at the end of 2022 and the emergence of more and more powerful competitive generative AI models throughout the period, the uptake of AI by EU companies accelerated significantly from 2023 to 2024.

Investments in AI

Quantitative estimates of the effects of AI on aggregate productivity are still uncertain. However, partial estimates point to significant gains. For example, benefits of USD 60-110 billion per year are estimated from the use cases of AI in the pharma and medical device industries. In the automotive sector, AI-powered (generative) algorithms can improve performance and reduce material use, reduce inventories, accelerate the time to market from R&I and increase labour productivity. AI uptake in freight and passenger transport will enable increasingly automated functions to deliver safety and quality and reduce fuel consumption. In the energy sector, where more than 50 use cases are already deployed today, ranging from grid maintenance to load forecasting, estimates of the market value for future AI applications reach USD 13 billion[80].

Following a slowdown in 2022 and 2023, AI investments have bounced back strongly. According to Dealroom, global venture capital investments in AI reached $124.9 billion in 2024, marking a 58 percent increase on 2023[81]; while private investments in AI in the EU grew by 22 percent in 2024 to USD 10.8 billion[82].

At the same time, the European Commission is multiplying its initiatives in favour of AI investment. At the AI Summit, President von der Leyen announced InvestAI, an initiative to mobilise EUR 200 billion for investment in AI in line with the political priorities of the Competitiveness Compass. This includes the launch of the InvestAI Facility, with a view to mobilising EUR 20 billion of investment for AI infrastructure, notably targeting up to 5 AI gigafactories across the EU. This builds on the creation of 13 AI Factories, with overall investments in supercomputing infrastructure and AI Factories in the EU that will reach EUR 10 billion over the 2021-2027 period.

Implementation of the AI Act

The speedy adoption of AI **systems requires legal certainty** for the entities in question. Other than the Data Union Strategy, which will help streamline the EU's legislative data landscape and identify measures to scale up the European data market, the EU has also taken steps to involve stakeholders and clarify the European Artificial Intelligence Act.

To facilitate the understanding of these provisions, on 4 February 2025 the European Commission adopted guidelines on prohibited practices, and on 6 February it adopted guidelines on the definition of an AI system. The guidelines on prohibited practices specifically address practices such as harmful manipulation, social scoring, and real-time remote biometric identification, among others. They are designed to ensure the consistent, effective, and uniform application of the AI Act across the

[80] Draghi, M., The future of European competitiveness, Part A – A competitiveness strategy for Europe, 2024.
[81] Dealroom, Artificial intelligence, 2024. Available at: https://app.dealroom.co/sector/technology/artificial intelligence/overview.
[82] Dealroom, Artificial intelligence, 2024. Available at: https://app.dealroom.co/sector/technology/artificial%20intelligence/overview?hqType=regions&hqValue=EU27.

European Union. While they offer valuable insights into the Commission's interpretation of the prohibitions, they are non-binding, with authoritative interpretations reserved for the Court of Justice of the European Union (CJEU). The guidelines provide legal explanations and practical examples to help stakeholders understand and comply with the AI Act's requirements. Although these guidelines and recommendations are non-binding, they are important stepping stones to ensure that companies interested in using AI can evaluate whether they are compliant with the AI Act. They are designed to evolve over time and will be updated as necessary, in particular in light of practical experiences, new questions and use cases that arise.

Boosting AI uptake

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

European Digital Innovation Hubs (EDIHs) play a key role in supporting effective AI integration by ensuring successful digital transformations of SMEs, small mid-caps and public sector organisations. Functioning as one-stop shops, they provide stakeholders with the opportunity to test AI solutions before investing in them, but also offer funding advice, networking opportunities, and training. From December 2025, EDIHs will place increased emphasis on AI uptake and ensuring adoption of AI solutions across sectors.

Additionally, a key measure is the GenAI4EU initiative, which takes a sectoral approach and has thus far allocated close to EUR 700 million in planned Horizon Europe and Digital Europe Programme calls.

GenAI4EU aims to stimulate the uptake of generative AI in a wide range of sectors, fostering collaboration between AI start-ups and deployers of AI in industry and the public sector. GenAI4EU is dedicated to unlocking the revolutionary potential of generative AI through ambitious projects, aiming notably to optimise production lines in manufacturing, improve robot autonomy and human-robot collaboration in complex tasks, and enhance our cyber defence and medical imaging capabilities.

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

In terms of actions, the Apply AI strategy will identify policy actions and concrete deliverables per sector, with key performance indicators to be achieved. Among others, the Commission will contribute to supporting developments through its funding programmes as well as through enablers

such as the AI Factories and Gigafactories, Data Spaces, Testing and Experimentation Facilities, European Digital Innovation Hubs, and AI Skills Academies, which will focus on sector-specific frameworks. This, in turn, will support AI uptake by European enterprises and the public sector.

Increasing the level of AI skills in the EU is one of the priorities that the Apply AI strategy will pursue, as an AI-literate workforce is necessary to boost AI uptake. Notably, the **AI Skills Academy** will function as a one-stop shop providing education and training on skills related to the development and deployment of AI, and in particular generative AI.

Finally, a candidate IPCEI in the field of AI is currently being designed. Interested Member States, with the support of the Commission services, are involved in the design phase where they explore the potential scope and structure of an IPCEI. This IPCEI candidate focuses on R&D&I and first industrial deployment activities aiming at developing groundbreaking AI technologies and services.

1.3 A secure continent

As geopolitical tensions deepen and the nature of conflict evolves, the intersection between digital innovation and defence has become a strategic imperative for the European Union. The war in Ukraine has exposed critical vulnerabilities and accelerated the EU's resolve to enhance its defence posture, while global technological competition – particularly in areas like artificial intelligence, quantum technologies, and secure connectivity – has underscored the urgency of investing in advanced capabilities. In this context, the EU is shifting towards a more integrated approach that connects digital policy with defence preparedness, recognising that Europe's security and strategic autonomy increasingly depend on its ability to develop, deploy, and govern cutting-edge digital technologies. At the same time, the EU is facing an intensifying cybersecurity threat landscape, marked by a surge in ransomware attacks, growing IoT vulnerabilities, and the targeting of critical infrastructure. This has prompted the development of a robust regulatory and policy framework to enhance cyber preparedness, promote resilience, and protect Europe's digital and physical assets. This chapter explores the emerging digital–defence nexus, outlining key trends, synergies, and policy initiatives shaping the future of a secure and sovereign Europe.

1.3.1 Digital-Defence nexus - Context and key trends

The European Union finds itself at a pivotal moment, confronting an increasingly volatile geopolitical environment. Since the Russian war of aggression against Ukraine in 2022, the EU and its Member States have committed to strengthening defence readiness and reinforcing the European Defence Technological and Industrial Base (EDTIB). The war in Ukraine, coupled with shifting global alliances and mounting geopolitical tensions, has underscored the imperative for Europe to bolster its own defence capabilities. The necessity for sustained military support to Ukraine, alongside the need to deter future aggressions, makes it clear that the EU must develop a robust, agile, and highly innovative defence industry to ensure long-term security and strategic autonomy.

Against this backdrop, the EU has taken significant steps to accelerate defence investment and enhance military preparedness. The White Paper for European Defence – Readiness 2030, published in March 2025, provides a political framework for these efforts, laying out the case for a surge in European defence investment. In particular, it identifies four strategic priorities for European defence readiness by 2030: increasing and sustaining support for Ukraine; closing critical defence capability gaps; promoting defence readiness through enhanced military mobility and stockpiling efforts; and strengthening the European defence industry by increasing demand predictability,

working towards simplification and accelerating the transformation of defence through disruptive technologies.

The latter point underpins a modern and adaptive defence industry, requiring an overarching approach to research, development and investment in transformative and disruptive technologies, in addition to the appropriate framework conditions necessary for an innovative defence industry ecosystem to develop.

To translate this vision into action, the ReArm Europe Plan is creating the conditions for an unprecedented surge in defence investment, enabling up to EUR 800 billion in defence expenditure over the coming years.

1.3.1.1 Synergies between Digital & Defence – Facts and figures

Digital technology and infrastructure are fundamental to enhancing the EU's defence capabilities and military edge. The Digital Decade Policy Programme, while primarily focused on the digital transformation, contributes significantly to strengthening the EU's security, defence, resilience and strategic autonomy. In particular, its focus on supporting the development of sovereign solutions for European digital infrastructures and advanced digital technologies is bound to directly contribute to the overall level of preparedness of the EU and its Member States.

There are some areas where the Digital Decade target, process and bodies provide vital support which is likely to produce positive spin-ins for EU security and defence. Of those areas, we should mention in particular:

Secure Connectivity (IRIS², 5G/6G, Sovereign Cloud Networks)

Robust and secure communication networks are essential for modern defence operations.

IRIS² is set to become the European Union's third flagship programme, providing secure satellite communications. The constellation is designed to enhance the EU's resilience and ensure seamless connectivity for Member States. IRIS² will help bridge existing connectivity gaps while safeguarding critical infrastructure. By providing robust and secure communication channels, IRIS² will prove instrumental for defence and military users – reducing reliance on third-country providers like Starlink and enhancing the EU's strategic autonomy.

The integration of 5G and emerging 6G technologies is poised to significantly enhance the European Union's defence capabilities. 5G networks offer high data rates and ultra-reliable low-latency communications, crucial for modern military operations, including intelligence, surveillance, and reconnaissance (ISR) systems. Looking ahead, 6G technology is expected to further revolutionise defence operations by enabling more reliable, high-speed, low-latency communications. This advancement will support critical defence applications such as robotics, autonomous systems, virtual reality training, and advanced sensing capabilities.

Additionally, sovereign cloud networks can ensure that sensitive defence data is stored and processed within the EU, maintaining data sovereignty and security. Sovereign cloud networks offer a crucial solution by, for example, providing a common, EU-based digital platform for integrating and operating naval systems (SOTS). These networks also facilitate predictive and prescriptive analytics, enhancing situational awareness and operational readiness.

Artificial Intelligence

Artificial intelligence is having a transformative effect on our society and economies. Equally, AI is having a significant impact on modern warfare, by enhancing decision-making, operational efficiency, and strategic autonomy.

AI-driven capabilities enable faster threat detection, improved situational awareness, optimised logistics, and greater precision in targeting. As global powers invest heavily in AI for defence, securing a technological edge is essential for the EU's security and resilience. Through the European Defence Fund (EDF), the EU is actively supporting AI research and development, making it a key enabler across multiple defence domains[83].

There is significant potential to leverage synergies between civilian and defence AI to accelerate innovation and enhance Europe's competitiveness and strategic autonomy in this critical domain. Initiatives such as AI Factories and EuroHPC could provide critical infrastructure for developing advanced AI models, supporting key defence applications such as real-time data processing, predictive analytics, and autonomous systems.

Semiconductors

Semiconductors are critical to the EU's digital transformation, and they are essential for defence capabilities, underpinning technologies in aerospace, communications, and security systems. The global semiconductor supply chain is highly sensitive and vulnerable to geopolitical tensions, with export controls such as the US International Traffic in Arms Regulations (ITAR) potentially limiting access to key technologies. As such, ensuring a secure and sovereign semiconductor production capacity for critical sectors, including defence, is a priority for the European Commission.

An example of leveraging EU civilian instruments for defence applications is NanoXplore, a French SME that developed NG-MEDIUM, the first fully European space-qualified Field-Programmable Gate Array, with support from Horizon Europe. Originally focused on space applications, NanoXplore has expanded into the defence sector, providing radiation-hardened components essential for military-grade electronics. This transition exemplifies how EU-funded technological advancements can enhance Europe's strategic autonomy in defence.

Quantum

Quantum computing holds the potential to revolutionise defence capabilities, particularly in cryptography, intelligence, and advanced simulations.

Quantum Key Distribution (QKD), supported by initiatives such as EuroQCI, can ensure ultra-secure military communications, reducing vulnerabilities to cyber threats.

Quantum sensing enhances geospatial intelligence, submarine detection, and inertial navigation, with projects like Carioqa-PMP and QSG Pathfinder paving the way for advanced surveillance and reconnaissance applications.

EU civilian instruments supporting the development of quantum technologies, such as the Quantum Flagship and Horizon Europe, can be leveraged for defence applications, fostering innovation in

[83] Examples include AIDEDex and CONVOY for AI-driven threat detection; AIDA and AInception for cybersecurity applications; or FaRADAI and KOIOS for AI-powered language processing in defence.

quantum-enhanced AI and supercomputing. These technologies support faster AI model training for defence applications and improve decision-making in complex operational environments. Quantum Space Gravimetry (QSG) can enhance Earth surface mapping and navigation accuracy, crucial for intelligence and surveillance. EU quantum supercomputers, developed under the EuroHPC Joint Undertaking, could support high-complexity defence applications.

Additionally, spin-in projects under the EDF, such as ADEQUADE and QuantaQuest, explore disruptive quantum solutions tailored for European defence needs.

Start-Ups and Unicorns: Driving Defence Innovation

A strong ecosystem of defence-tech start-ups and SMEs is critical for Europe's ability to develop and scale up cutting-edge defence technologies. Recent EU initiatives have sought to strengthen this ecosystem by providing dedicated support and investment opportunities for companies developing defence and dual-use technologies, while the Digital Decade's strong and continued focus on the development of start-ups and unicorns proved to be vital in supporting a competitive and thriving ecosystem.

The launch of the EUDIS Matchmaking and Business Accelerator programmes marks an important step in supporting EU start-ups and SMEs, including those focused on dual-use technologies. The EU is also mobilising investment through key funding instruments. As announced in the White Paper on the Future of European Defence, the European Innovation Council (EIC) and the TechEU Scale-up Fund will provide financial backing to companies working on dual-use technologies, helping them scale up and compete globally.

Investment in defence is further supported by major policy shifts at the European Investment Bank (EIB). The recent revision of the EIB's exclusion policy signals a commitment to stepping up investment in security and defence-related projects, thereby addressing longstanding funding gaps in this sector. These efforts ensure that EU start-ups remain at the forefront of innovation in critical digital technologies with defence applications.

1.3.1.2 Key measures taken at EU level in 2024

In 2024, the European Commission took several steps to support digital technologies for defence.

In January 2024, the European Commission launched, through the European Investment Fund (EIF), the EUR 175 million Defence Equity Facility. This facility targets venture capital and private equity funds investing in European companies developing innovative defence technologies with dual-use potential. The initiative seeks to stimulate private investment, aiming to leverage approximately EUR 500 million in total funding. To date, two investment deals have been signed, with two more expected by the end of the year.

Throughout 2024, the European Commission continued to support defence innovation through various programmes. The EDF financed projects focused on critical digital technologies such as AI, quantum technologies, cloud solutions, and secure communications. These projects aim to enhance operational effectiveness and technological advancement within the defence sector.

In parallel, Technological Challenges took place under the EDF to foster innovation and problem-solving within the defence community. The 2024 challenge topics addressed pressing defence needs, including robust autonomous drone navigation and multi-source satellite image analysis.

The Commission launched EUDIS Hackathons. Under the theme 'Digital in Defence', the first Hackathon was held from 31 May to 2 June 2024. It took place simultaneously across 6 European countries (Belgium, Greece, Hungary, Italy, Lithuania, and Poland), gathering 275 participants from 16 countries, 79 mentors and experts, and 6 winning teams. This initiative sparked the creation of 70 cutting-edge ideas and innovative solutions in the defence sector.

The event focused on enhancing Europe's defence capabilities in three challenge areas: Subsea Infrastructure Protection, Improving Situational Awareness, and Cybersecurity in Defence. The next edition will take place in 2025, under the topic *Rapid Defence Solutions for the Ukrainian battlefield and beyond.*

In March 2025, the EU published the White Paper for European Defence and the ReArm Europe Plan/Readiness 2030. The White Paper outlines strategic priorities for defence technology investments, identifying AI, quantum technologies, cybersecurity, and electronic warfare as key capability domains requiring focused investment. Additionally, the White Paper proposes the development of a European Armament Technological Roadmap in 2025, leveraging investments in key technologies with dual-use potential, with an initial focus on AI and quantum.

This initiative is complemented by ProtectEU, the European Internal Security Strategy, which aims to increase Member States' capabilities to protect societies and democracies from online and offline threats, as well as the Preparedness Union Strategy, which will boost the EU's ability to anticipate, prevent, and respond to the threats faced by the EU.

Collectively, these initiatives underscore the EU's commitment to advancing digital transformation in defence, ensuring that technological progress translates into enhanced security and strategic autonomy.

1.3.1.3 Investment needs/investment gaps

The EU's defence sector has faced decades of underinvestment, with a cumulative defence spending gap of over EUR 1.25 trillion from 2006 to 2022. This has resulted in a lack of necessary capabilities and modernisation across the European Defence Technological and Industrial Base (EDTIB)[84]. The recently adopted ReArm Europe Plan/Readiness 2030 aims to address these gaps by mobilising up to EUR 800 billion in defence investments. This includes SAFE, which provides EUR 150 billion in loans for joint defence projects, and greater flexibility within the Stability and Growth Pact, allowing Member States to increase defence spending without breaching fiscal rules. These measures will help to create a more supportive environment for boosting defence investment across the EU.

SMEs and start-ups developing defence and dual-use technologies are particularly affected by these funding gaps[85], with defence start-ups still facing significant challenges in accessing finance, especially during growth stages. Many of these companies report difficulties in accessing traditional financial instruments, with close to 40% of defence SMEs indicating that they find access to finance difficult or very difficult[86].

Several barriers hinder private sector investment in the EU defence sector:

---

[84] European Commission, Defence Investment Gaps Analysis and Way Forward, 2024.
[85] Dealroom.co & NATO Innovation Fund, Defence, Security and Resilience in Europe: The state of start-ups and venture capital, 2025.
[86] European Commission, Access to equity financing for European defence SMEs, 2023.

- **Exclusion policies:** historically, the EIB and EIF exclusion policies limited investments in certain defence activities. However, following the adoption of the EU's White Paper on Defence – Preparedness 2030, these policies have been updated, which should help reduce the barriers to private investment.
- **Ethical and regulatory concerns:** private investors have often been deterred by ethical concerns and regulatory uncertainties surrounding defence-related investments, especially in relation to ESG criteria.
- **Lack of defence-specific financial instruments:** the EU lacks a well-developed ecosystem of defence-focused venture capital and private equity funds. The launch of the Defence Equity Facility (DEF) under InvestEU is a step in the right direction, providing financial support to private funds investing in defence technologies, particularly those with dual-use potential. As announced in the White Paper, investment in dual-use companies by the EIC and TechEU Scale-up Fund is also expected to address some of these financing gaps.
- The EIB is preparing a study titled 'Analysis of the market gap for growth stage funding in strategic technologies and identification of funding sources for an initial set of potential investments'. It will offer further insights into the specific funding gaps in the defence sector and provide recommendations for improving access to finance for defence companies.

1.3.1.4 The way forward

In light of the evolving geopolitical landscape and the changing nature of warfare, the Commission's efforts to integrate digital technologies into defence remain critical for enhancing the EU's security and defence capabilities. Existing civilian-focused initiatives have laid the foundations for leveraging cutting-edge digital technologies – including AI, quantum technologies, and semiconductors – to strengthen defence capabilities. However, challenges remain, including the need to deepen integration between defence and digital policy, address gaps in digital infrastructure, and accelerate innovation in critical technologies.

To build on current momentum, we should further leverage EU civilian-focused instruments and investments in dual-use technologies to support defence priorities. The Commission should also step up investment in emerging technologies with dual-use potential and ensure that both digital and defence policies are aligned. A more coordinated approach will be key to enhancing EU preparedness in the face of evolving threats.

The Commission's recent White Paper on European defence recognises the profound transformation that the defence landscape is undergoing, driven by the rapid evolution of new technologies and the global technology race: technologies like AI, cloud and quantum computing, advanced and secure connectivity, autonomous systems and alternative energy sources have the capacity to disrupt and transform traditional approaches to warfare. The White Paper also points out that the EU's strategic competitors, including Russia and China, are investing heavily in military innovation. As a response, the White Paper proposes the development of a **European Armament Technological Roadmap** in 2025, which will identify key defence technologies and leverage investments in dual-use advanced technological capabilities, initially focusing on critical areas such as AI and quantum.

Major strategic-level documents have also pointed at the key trends and contributions that digital technologies could bring to the defence and security sectors, highlighting the potential for

maximising the impact of investments, the risks stemming from new and disruptive technologies, and the opportunity for their integration in new security and defence applications[87].

The structured cooperation process established by the Digital Decade Policy Programme, along with its multi-level governance system, holds substantial potential to advance the objective of strengthening security and defence in the EU, while fostering security culture across EU digital policy sectors. Building on the Digital Decade method and processes would facilitate and promote a 'whole-of-government' and 'whole-of-society' approach to addressing security challenges and defence readiness, as advocated by the Niinistö report. Moreover, the Digital Decade Policy Programme could provide valuable input and support the development of the proposed European Armament Technological Roadmap.

The Digital Decade Policy Programme could contribute to EU security & defence efforts in several key areas:

- Supporting innovative actors, including start-ups proposing disruptive digital applications and services, and connecting the defence and digital innovation communities.
- Assisting Member States in developing digital infrastructures that contribute to societal resilience in crisis contexts.
- Fostering a new mindset towards preparedness and security culture across the digital sector.
- Identifying synergies between defence and digital programmes, investments, and applications.

1.3.2 Cybersecurity

1.3.2.1 The cybersecurity threat landscape in 2024

Cyber threats continue to evolve at an alarming pace, with increasingly sophisticated attacks targeting critical sectors and exploiting emerging vulnerabilities. In 2024, the healthcare sector was particularly affected, with ransomware accounting for 71% of cyber incidents impacting patient care in the EU, leading to delayed treatment and diagnosis, and restricted access to emergency services[88]. Supply chain attacks have also surged, as cybercriminals exploit weaknesses in third-party vendors and service providers, while nation-state actors intensify politically motivated cyber espionage and infrastructure disruptions.

---

[87] Draghi, M., The future of European competitiveness, 2024. In particular on the digital contribution to defence: '(…) a weak tech sector will hinder innovation performance in a wide range of adjacent fields, such as pharma, energy, materials and defence'; Niinistö S., Safer together: strengthening Europe's civilian and military preparedness and readiness, 2024 Niinisto report: 'The wider set of dual-use infrastructures and capabilities that become vital in a war or crisis require an urgent upgrade. (…) This report has also flagged further dual-use opportunities in relation to space, critical infrastructure, maritime, communications, cyber, etc. within legal and regulatory margins. Moreover, a cultural shift is required within the EU to mainstream civil-military synergies and dual-use potential, rather than keeping defence-related applications and requirements separated from civilian innovation and broader funding options. We simply cannot afford to pay for these artificial limitations any longer'; Competitiveness Compass for the EU, COM(2025) 30 final; Joint Communication 'A new European Defence Industrial Strategy: Achieving EU readiness through a responsive and resilient European Defence Industry', JOIN (2024), defence industry.

[88] Joint Research Centre, Cybersecurity in the Health and medicine sector, 2024.

The growing use of IoT and operational technology (OT) devices in cyberattacks further complicates the threat landscape, with IoT malware increasing by 107% in the first half of 2024, and compromised devices enduring an average of 52.8 hours under attack[89].

Meanwhile, ransomware attacks rose by 11% compared to 2023, but enforcement actions against major groups like LockBit have led to a more fragmented threat environment, with 46 new ransomware groups identified in 2024[90]. These developments underscore the need for stronger cybersecurity measures, enhanced threat intelligence, and coordinated efforts to mitigate risks.

ENISA's '2024 Report on the State of Cybersecurity in the Union' reveals concerning trends in public cybersecurity awareness, with declining confidence among EU citizens in their ability to protect themselves from cybercrime and generally low awareness about reporting mechanisms. The report also highlights a significant cyber hygiene gap between SMEs and large enterprises.

ENISA has developed the 'AR-in-a-Box' toolkit providing organisations of all sizes with resources to create tailored cybersecurity awareness programs to enhance their security culture. It has also conducted targeted awareness campaigns over the past three years (2022-2024) for specialised audiences in the energy, healthcare, and transport sectors. Simultaneously, the agency launched the CyberALL campaign focused on promoting cybersecurity roles and enhancing inclusion within the field, further demonstrating a comprehensive approach to building cybersecurity awareness across different sectors and demographics.

Beyond organisational awareness, the report also identified disparities in cybersecurity education across Member States and emphasises the critical need to strengthen the EU cyber workforce through the Cybersecurity Skills Academy, with ENISA playing a key role through its development and promotion of the European Cybersecurity Skills Framework (ECSF), which benefits various sectors while also piloting an innovative cybersecurity skills attestation scheme designed to further harmonise and enhance the EU cybersecurity landscape.

ENISA's May 2024 Cybersecurity Education Maturity Assessment shows progress, with 78% of Member States now providing cybersecurity education to primary and secondary school pupils, reaching a 66% overall maturity level. To further harmonise these efforts, ENISA's CyberEdu platform centralises standardised resources and frameworks that can be adopted across the EU, supporting a more unified approach to cybersecurity education and awareness.

The European Cybersecurity Month (ECSM) has served as a cornerstone initiative for cross-Member State collaboration in cybersecurity awareness. Since 2012, ECSM has united diverse stakeholders under 'Cybersecurity is a Shared Responsibility,' and this has proven effective, with the campaigns reaching over 47 million EU citizens in 2023 through its network of more than 300 partners from governments, universities, think tanks, and businesses across all Member States.

1.3.2.2 Cybersecurity in enterprises

When it comes to cybersecurity in enterprises, according to Eurostat, 92.76% of surveyed enterprises in the EU with more than 10 employees and self-employed persons used at least one ICT security measure in 2024.

---

[89] SonicWall 2024 Mid-Year Cyber Threat Report, 2024.
[90] Cyberint platform, 2025, Ransomware Annual Report 2024.

However, for specific individual measures the figures were lower: for example, only 35.50% of the enterprises had documents on measures, practices or procedures on ICT security, and only 34.10% of the enterprises had used an ICT risk assessment. Commonly used measures included strong password authentication (83.69% of enterprises) and data backups in a separate location (79.23% of enterprises). According to Eurostat, 21.54% of enterprises experienced ICT-related security incidents leading to some consequences in 2023.

Under the NIS Directive, the NIS Cooperation Group has published annual reports on the number of cybersecurity incidents reported. The latest available report covers the year 2023, showing that the total number of incidents reported under the NIS Directive was 1 077 – an increase from the 890 incidents reported in 2022. For the fourth consecutive year, the health sector reported the most incidents (309), followed by the transport (209) and banking (149) sectors.

The NIS Investments Report, published annually by ENISA, assesses the overall cybersecurity maturity level of entities in critical sectors. The 2024 NIS Investments Report found that the median level of information security spending among the surveyed organisations was 9.0% of overall IT spending, an increase of 1.9 percentage points compared to the previous year. Furthermore, the report found that on average, organisations already covered by the NIS Directive perceived themselves as more mature in terms of cyber risk management, network and information security arrangements and cyberattack detection and response capability, compared to organisations in sectors newly covered by the NIS2 Directive.

ENISA's 2024 Report on the State of Cybersecurity in the Union, published pursuant to Article 18 of the NIS2 Directive, displays the overall level of cybersecurity maturity of 10 critical sectors and sub-sectors based on a methodology developed by ENISA. The report finds that the telecommunications sector has the highest level of maturity, while the oil sector's maturity is the lowest. Among other recommendations, the report proposes that Member States assess and monitor the maturity and criticality of sectors at national level, and that they conduct national risk assessments of selected sectors.

Insight internet standards adoption

Globally agreed Internet standards are at the core of the evolution of the Internet and by extension of the digital economy and society. The deployment of the latest available standards not only adds enhanced or new features to the Internet infrastructure, but in many cases also brings crucial improvements to cybersecurity. Hence, following the 2020 communication 'The EU's Cybersecurity Strategy for the Digital Decade' and the 2022 standardisation strategy 'An EU Strategy on Standardisation Setting global standards in support of a resilient, green and digital EU single market', the Commission biannually publishes deployment data for several categories of cybersecurity-relevant key internet standards and best practices. The data is published on the EU Internet Standards Deployment Monitoring Website and consolidates publicly available data and its own measurements based on an empirical approach by the Commission's Joint Research Centre. **The data shows slow and/or incomplete deployment rates for several Internet standards, which deliver very basic and crucial security features and Internet functionalities, despite their well-accepted benefits**. This undermines trust in, and the resilience of the Internet as a crucial infrastructure for societies and economies. The slow transition from IPv4 to IPv6, the latest version of the Internet's underlying work horse, stifles innovation due to the depletion of IPv4 addresses and creates and perpetuates a double attack surface. The current user-side and server-side IPv6 adoption rates in the EU are roughly 36.4% and 16.8% respectively, which is only a little ahead of the average global

adoption rate. The adoption rate is steadily increasing both globally and in the EU, though at a very slow pace for the EU. In particular, the user-side adoption rate is highly fragmented across Member States, with Belgium, France, Germany, Greece, Hungary, and Portugal in the lead (>40%) and Croatia, Cyprus, Malta, Slovakia, and Spain lagging behind (<10%).

Another example are the Domain Name System Security Extensions (DNSSEC). The Domain Name System (DNS) attributes human-readable names to IP addresses. It is one of the most critical parts of the internet infrastructure. DNSSEC are a suite of specifications that improve the security of DNS. Based on Q3 2024 data, the DNSSEC validation rate by resolvers in the EU reaches 47.5% and hence is higher than the global rate which scores approximately 32.5%. The validation rate is trending upward, but at very slow pace. Similarly to IPv6, the values are fragmented across Member States. Overall, the values are clearly insufficient to achieve the benefits of DNSSEC deployment.

1.3.2.3 Key measures taken in 2024/2025

The EU has taken significant steps in 2024 and early 2025 to strengthen cybersecurity across all sectors. Among the key developments, the NIS2 Directive, adopted in December 2022, sets cybersecurity risk management and incident reporting requirements for essential and important entities in 18 critical sectors. On 17 October 2024, the Commission adopted an implementing act detailing technical and methodological requirements for risk management and incident reporting in digital infrastructure, digital services, and B2B ICT service management. As the transposition deadline for Member States passed on the same day, the Commission launched infringement procedures in November against 23 Member States that failed to comply, while continuing to support the transposition process.

Further reinforcing cybersecurity, the Cyber Resilience Act introduces mandatory cybersecurity requirements for hardware and software products on the EU market. It entered into force on 10 December 2024 and includes a three-year transition period, with reporting obligations starting in September 2026 and full implementation in December 2027. To facilitate its roll-out, an expert group has been established, and a standardisation request has been issued to European Standardisation Organisations. The Commission is also preparing an implementing act to define critical product categories and a delegated act setting conditions for cybersecurity-related notifications. Additionally, ENISA is working on a single reporting platform where manufacturers will report vulnerabilities and severe security incidents.

Another major step was the entry into force of the Cyber Solidarity Act on 4 February 2025, establishing the European Cybersecurity Alert System, the EU Cybersecurity Emergency Mechanism, and the Cybersecurity Incident Analysis Mechanism. The Alert System will rely on a network of National and Cross-border Cyber Hubs to enhance cyber threat detection and situational awareness using advanced technologies like AI. The Emergency Mechanism will build preparedness and response capabilities, including an EU Cybersecurity Reserve of trusted providers to assist in handling large-scale cyber incidents. A dedicated Incident Review Mechanism will also assess significant cyber threats and incidents.

The European cybersecurity certification framework was further strengthened with an amendment to the Cybersecurity Act, published in January 2025 and effective since 4 February. This amendment expands the scope of certification to include managed security services, bolstering protection for industries, citizens, and critical infrastructure. Additionally, a new implementing regulation adopted in December 2024 establishes a process for notifying conformity assessment bodies through the

NANDO information system. The Commission has invited Member States to designate their National Cybersecurity Certification Authorities accordingly.

Despite the robust framework provided by the 5G Toolbox to secure 5G networks, many Member States have yet to impose necessary restrictions on high-risk suppliers, leading to persistent strategic dependencies. This situation increases the risk of interference by non-EU countries and could impact future 6G infrastructure, which will be built on existing 5G networks. To address this, Member States must fully implement the 5G Toolbox without further delay, while the Commission is exploring additional legislative measures to enhance internal market resilience.

Cybersecurity in healthcare has also become a priority, with the new Commission's Political Guidelines announcing an EU action plan to improve cyber threat detection, preparedness, and crisis response for hospitals and healthcare providers. Adopted on 15 January 2025, the plan includes tailored guidance, tools, services, and training to reinforce cybersecurity in the sector.

In February 2025, the Commission put forward a proposal for a Council Recommendation on a Cybersecurity Blueprint, updating the 2017 framework to reflect legislative and institutional changes. The revised Blueprint strengthens cooperation among Member States and EU entities in managing large-scale cyber incidents and integrates cyber crisis response into the broader EU crisis management framework. It enhances shared situational awareness and coordination between civil and military cybersecurity actors. The Council Recommendation was adopted in June 2025.

Work is also progressing on the European Quantum Communication Infrastructure (EuroQCI), which is integrated into the Union Secure Connectivity Programme (IRIS^2). EuroQCI will provide highly secure quantum-enhanced encryption for public administrations and critical infrastructure, such as hospitals and energy grids. Throughout 2024, efforts focused on deploying national quantum communication networks, advancing key European technologies, and preparing for the deployment of quantum communication in space. Eagle-1, Europe's first quantum communication satellite, is set to launch in 2026. While EuroQCI will mitigate some risks posed by quantum computing to current encryption methods, the transition to post-quantum cryptography (PQC) remains essential. To guide this transition, the Commission published a recommendation in 2024 outlining a coordinated roadmap, working with Member States to secure digital infrastructure and services against emerging cyber threats. Germany's federal cyber security authority (BSI), together with representatives of 17 other Member States, published a joint statement on post-quantum cryptography in November 2024, advocating for industry, critical infrastructure providers and public administration to start the transition to PQC.

1.3.2.4 Investment needs and market trends

At EU level, to date, dedicated funding for cybersecurity is provided by Horizon Europe and Digital Europe Programmes, in the form of grants. InvestEU provides limited funding for cybersecurity, and in competition with other digital technologies.

The aim of EU funding is to strengthen EU technological sovereignty, develop the European cybersecurity market to make it more competitive on the global landscape, and enhance European strategic autonomy in cybersecurity, ultimately making the European Union more cyber resilient. EU funding is also instrumental in supporting industry, particularly SMEs, in their uptake of EU cyber legislation, such as NIS2 and the Cyber Resilience Act (CRA).

The European Cybersecurity Investment Platform study of October 2022 released by the EIB provides an extensive analysis of the European investment landscape in cybersecurity and compares it with

major competitors worldwide. Despite being released at the end of 2022, the study and its quantitative analysis remain extremely relevant: the study reports that the current provision of financing for cybersecurity projects in the European Union is limited to only a few specialised funds actively investing in this sector. In fact, in 2021 venture capital investments in cybersecurity in Europe amounted to about **EUR 814 million, compared with over EUR 15 billion in the United States and EUR 2.5 billion in Israel**.

In addition, **70% of the EU's supply of cybersecurity venture capital is concentrated in four Member States** – namely France, Germany, Italy and Spain – and, according to consulted stakeholders, there is little cross-border investment, thus hindering the emergence of larger funds.

To address the investment gap, the study suggests various solutions, one of which is to strengthen public-private partnerships combining various resources, including from the European Commission, the EIB, national investment funds, national cybersecurity funds, and private sector investors. The EIB study also highlights the lack of data on the cybersecurity sector. The scarcity of data is a barrier for more investors to enter the market, as they struggle to make informed investment decisions.

To address the public availability of EU cyber market data, the Commission, through the European Cybersecurity Competence Community (ECCO) procurement contract led by ECSO (European Cyber Security Organisation), has recently developed a data platform on the European Cybersecurity Market (ECCO Market Observatory). It will soon be available to the public on the European Cybersecurity Competence Centre website. Such a data platform could be of benefit to a variety of stakeholders, including investors.

Insights derived from the ECCO Market Observatory show that the **EU cybersecurity ecosystem generates around EUR 67 billion** and consumes around EUR 65 billion each year, with encryption being the largest sector in Europe. The main activity in cybersecurity is the provision of services which, at EUR 48 031 billion, accounts for 72% of total sales, followed by software development and production at 13% and consulting at 12%.

The main EU consumers of cybersecurity products and services are the insurance sector (EUR 5 billion/7.7%), followed by ICT (EUR 4.9 billion/7.5%), financial services (EUR 4.6 billion/7.0%) and government (EUR 4.3 billion/6.6%).

Trade between Member States is significant and comprises over 10% of production in all Member States. Import/export figures with the rest of the world indicate that the EU, in financial terms, consumes roughly what it produces with possibly a slight trade surplus.

1.3.2.5 Conclusions

In sum, 2024 and early 2025 have marked a pivotal period in strengthening the EU's cybersecurity landscape. Faced with a rapidly evolving threat environment – driven by ransomware, IoT vulnerabilities, supply chain risks, and geopolitical tensions – the EU has responded with an ambitious and multifaceted policy agenda. Key legislative instruments such as NIS2, the Cyber Resilience Act, and the Cyber Solidarity Act are reshaping the regulatory and operational framework, while ENISA's expanding role supports harmonisation, awareness, and skills development. Persistent challenges remain, notably in closing the investment gap, fostering cross-border financing, and ensuring full and timely implementation across Member States.

2 Protect and empower people, preserve EU democracy and values

The digital transformation is a key driver for building a fair, inclusive and secure society in line with the European Declaration on Digital Rights and Principles[91]. A people-centred digital decade requires not only boosting technological capacity and economic competitiveness but also strengthening societal resilience, democratic integrity, and individual empowerment in a fast-changing digital landscape.

Ensuring that all people can meaningfully participate in the digital world requires investment in both basic and advanced digital skills, from everyday literacy to cutting-edge expertise in AI, cybersecurity and semiconductors. Strengthening Europe's digital talent base is essential for supporting innovation, closing social and territorial divides, and equipping citizens for an evolving labour market shaped by technological disruption.

At the same time, achieving an inclusive digital society based on trust depends on the ability to provide secure, interoperable and user-friendly public services that are accessible across borders and designed around people's needs. This requires efforts to improve transparency, reduce administrative burden and foster more connected and efficient digital public infrastructures.

In parallel, rising systemic risks–ranging from illegal and harmful content and addictive design to information manipulation by foreign actors–highlight the need for stronger protections in the digital space. Ensuring the safety and well-being of users, particularly children, and safeguarding the integrity of information and of democratic processes is essential to upholding fundamental rights in the EU and preserving social trust. Together, these efforts shape a digital environment rooted in inclusive participation and democratic values.

This chapter presents the progress made toward the Digital Decade targets in these areas, highlights structural gaps, and outlines key policy levers for a digital transformation that empowers individuals and strengthens democratic resilience.

2.1 Empower people through digital skills

2.1.1 Equip people with at least basic and above basic digital skills

In today's digital world, basic digital skills and literacy are essential for both economic participation and civic engagement. These skills are necessary not only for employment–where most job roles require some level of digital competence for effective performance and adoption of emerging technologies–but also for navigating a wide range of online services such as shopping, banking, and e-voting. They are also crucial for engaging in lifelong learning opportunities, including online courses, and for developing safe and responsible online habits to guard against risks such as phishing, fraud, and disinformation.

[91] While reference is sometimes made to the Declaration on Digital Rights and Principles in this Chapter, the SWD 'Monitoring of the European Declaration on Digital Rights and Principles, SWD(2025) 293, https://digital-strategy.ec.europa.eu/en/policies/2025-state-digital-decade-package, presents action taken in this respect at both European and national level.

Bridging the digital divide is therefore critical for ensuring that all Europeans have **fair and equal access** to education and training in basic digital skills. This is not only key to achieving a **human-centric, secure, and sustainable digital transformation** but also to **securing quality jobs**, fostering **an inclusive society**, protecting **democracy**, and upholding **EU values**. The Declaration on Digital Rights and Principles includes a number of commitments made by Member States on digital education, training and skills (e.g. promoting high-quality digital education and training, including with a view to bridging the digital gender divide, giving everyone the possibility to adjust to changes brought by the digitalisation of work through up-skilling and re-skilling etc).

As digital technologies become more pervasive, people are interacting daily with **algorithms embedded in social media, search engines, and shopping platforms**, often without realising how these systems shape what they see, what they choose, and how they think. The growing presence of **general-purpose AI** in everyday life–from work to education and communications–further reinforces the importance of **algorithmic awareness and AI literacy**. These skills are essential for identifying bias, recognising misleading or false information, and understanding how personalised content can influence not only consumer choices but also democratic processes. Finally, greater awareness of one's **digital footprint** also plays an important role in promoting more sustainable digital behaviours and supporting **environmental goals**.

Progress towards the Digital Decade target

Target: A digitally skilled population and highly skilled digital professionals, with the aim of achieving gender balance, where (a) **at least 80% of those aged 16-74 have at least basic digital skills.**

KPI definition (referring to part (a) of the target): At least basic digital skills, measured as percentage of individuals aged between 16 and 74 years old disaggregated by sex with 'basic' or 'above basic' digital skills in each of the following five dimensions: information, communication, problem solving, digital content creation and safety skills. It is measured based on the activities that individuals carried out during the previous three months[92]; and gender convergence, measured as the percentage of women and men among those individuals with 'basic' or 'above basic' digital skills.

Source: Eurostat, European Union survey on ICT usage in households and by individuals.

Available data points: 2015, 2016, 2017, 2019, 2021, 2023 (break in series in 2021).

2023 data values: 55.6%

The percentage of people with at least basic level of digital skills rose by a mere 1.7 percentage points in two years, from 53.9% in 2021 to 55.6% in 2023. This represents a year-on-year increase of 1.5%.

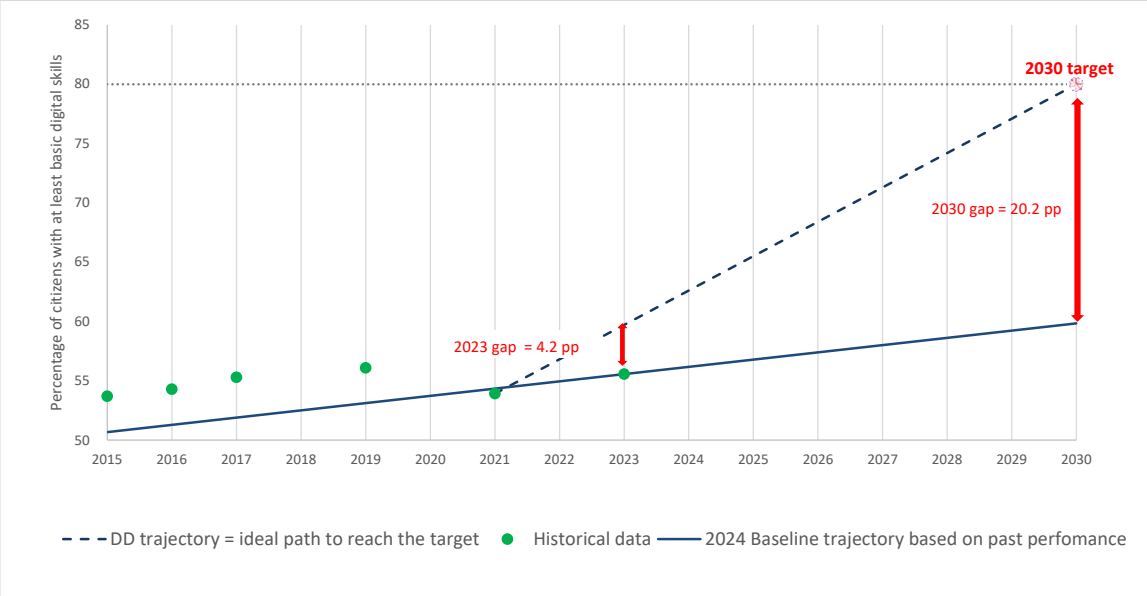
In 2024, the percentage of people with at least basic level of digital skills **stood at 93% of the ideal value along the digital decade trajectory** (55.6% instead of 59.7%). The gap between the forecast value and the ideal one is expected to widen until the end of the decade.

[92] Defined based on the Eurostat methodology reflecting the revised Digital Competence Framework (DIGCOMP 2.0), as also set out in Commission Implementing Regulation (EU) 2022/1399 of 1 August 2022 specifying the technical items of the data set, establishing the technical formats for transmission of information and specifying the arrangements and content of the quality reports on the organisation of a sample survey in the use of information and communication technologies domain for the reference year 2023 in accordance with Regulation (EU) 2019/1700 of the European Parliament and of the Council.

According to the forecast along the baseline trajectory, only **74.8% of the target will be achieved by 2030**, reaching 59.8% instead of 80%.

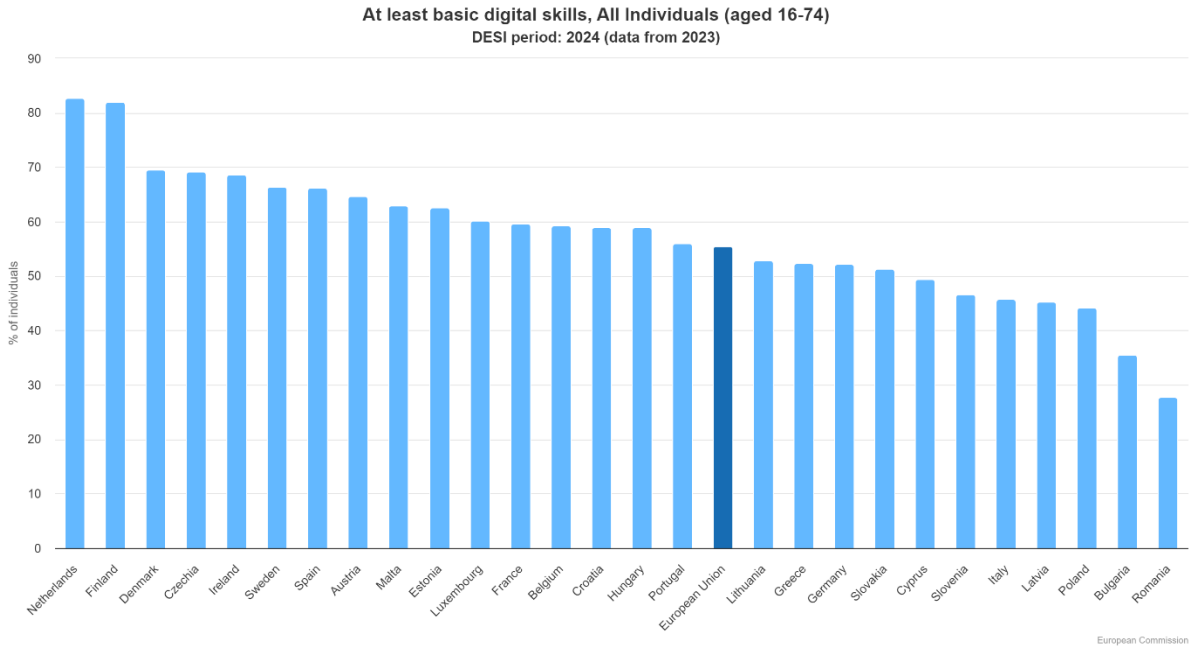
At this very slow pace of progress, the full target is forecast to be reached not earlier than in **2063** if no further actions are taken.

Figure 26: At least basic digital skills in the EU. Historical data, Digital Decade (DD) trajectory and revised baseline trajectory towards 2030



<u>Basic digital skills in the EU: gaps, disparities</u> and **<u>risk factors</u>**

Figure 27. At least basic digital skills. DESI period 2024 (data from 2023).



While the EU has made progress in expanding access to digital technologies, the distribution of basic digital skills remains uneven across population groups and Member States. Evidence from recent surveys and studies highlights a persistent divide between those equipped to participate fully in the digital world and those at risk of exclusion. This section presents key data points that illustrate the

scope of the challenge, examining digital skill gaps by age, education, socio-economic status, and labour market participation, as well as mismatches between supply and demand in the labour market.

Many school-age children lack essential digital competences. The 2023 International Computer and Information Literacy Study (ICILS)[93] found that 43% of 13 to 14-year-olds across 22 EU education systems did not possess a basic level of digital skills. Large disparities were observed across countries, socioeconomic statuses, and migrant backgrounds. While Czechia and Denmark performed well, Romania and Greece significantly underperformed.

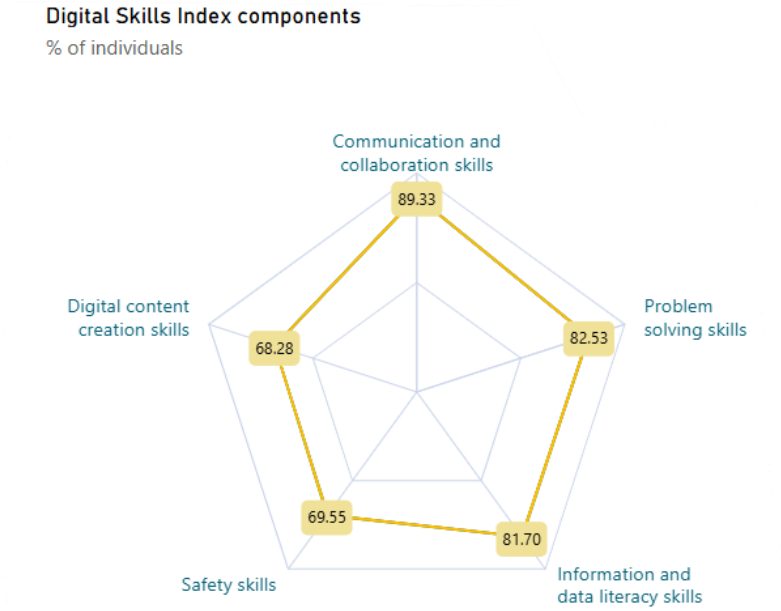
Home resources play a defining role in student outcomes. The ICILS data highlight how unequal access to digital tools and parental support at home shapes students' digital performance. In this context, schools must function as equalisers, helping level the playing field through adapted curricula, teacher support, and targeted resources. Closing this gap is essential for preparing students for academic success and active participation in a digital economy and society.

Educational attainment remains a strong predictor of digital skills. According to the DSI 2.0[94], in 2023, the gap in at least basic digital skills between individuals with a high level of formal education and those with little or no formal education was 46.2 percentage points. Ireland, Portugal, and Greece exhibited the largest disparities, with gaps of 73.8, 65.6, and 63.1 percentage points, respectively. In contrast, Estonia, Finland, and Lithuania displayed the smallest disparities at 11.6, 13.9 and 22.2 percentage points, respectively.

Specific skill areas remain underdeveloped. Individuals are assumed to possess digital skills when they engage in an online activity or software use. The DSI suggests that digital content creation and safety skills are the weakest areas, indicating gaps in programming skills, data handling, and basic cybersecurity practices.

[93] 2023 International Computer and Information Literacy Study
[94] Digital Skills Indicator 2.0, EU survey on the use of ICT in households and by individuals, 2023.

Figure 28. Digital Skills Index components.



Labour market demand remains concentrated and uneven. A Joint Research Centre (JRC) exploratory study[95] using the European database on online job advertisements (OJA) found that 27% of job postings required at least one digital competence of the Digital Competence Framework for Citizens (DigComp)[96]. The highest demand was for skills in information and data literacy, content creation, and collaboration. However, safety-related skills were rarely mentioned, revealing a possible disconnect between labour market expectations and the broader societal need for secure digital engagement.

Older generations continue to lag behind. Across the EU, there is a 41.8 percentage point gap in at least basic digital skills between individuals aged 16-24 and those aged 65-74. The difference is especially pronounced in Malta, Croatia and Czechia (74.2, 68.4, and 67.1 percentage points respectively), mainly due to higher levels of digital competence among younger adults. Luxembourg, Ireland and Germany record the smallest age-related disparities[97].

Vulnerable demographic groups face compounded disadvantages. Another JRC study[98] has identified young people (aged 16-24) with low educational attainment, manual workers, and those unemployed or outside the labour market as highly likely to lack basic digital skills. For instance, young people aged 16-24 with low education face a 43% probability of being digitally excluded. This

---

[95] Joint Research Centre, Cosgrove, J et al, Mapping DigComp digital competences to the ESCO skills framework for analysis of digital skills in EU online job advertisements | European Skills, Competences, Qualifications and Occupations (ESCO), 2024.

[96] Joint Research Centre, Digital Competence Framework for Citizens (DigComp) The Digital Skills indicator, based on the Digital Competence Framework for Citizens (DigComp 2.2) measures 12 key competences across five areas: Information and data literacy, Communication and collaboration, Digital content creation, Safety, and Problem solving.

[97] State of the Digital Decade 2024 report

[98] Joint Research Centre, Bertoni, E et al, JRC Publications Repository - Digital skills gaps - a closer look at the Digital Skills Index (DSI 2.0), 2025. The findings are based on a multivariate analysis conducted by the Joint Research Centre (JRC) examining the Digital Skills Indicator and the specific competencies it measures.

is compounded by low participation in digital citizenship and low levels of data skills, cybersecurity literacy, and online learning.

The above findings highlight a considerable risk of digital exclusion among younger generations and vulnerable groups. As threats of cybersecurity breaches and disinformation grow, EU initiatives promoting citizen cyber skills and fostering cybersecurity and cyber literacy in schools are more relevant than ever. At the same time, the data emphasises the need to support digital lifelong learning and ensure that access to digital skills training is accessible to all segments of society. Bridging the digital divide will be essential for reducing the proportion of low achievers in computer and information literacy (CIL) to less than 15% by 2030, in line with EU targets, and for ensuring that no one is left behind in Europe's digital transformation.

Supporting basic digital skills through EU-level initiatives

To accelerate progress towards the 2030 Digital Decade targets, the EU has introduced a comprehensive policy and investment framework aimed at strengthening digital skills across society. These measures are designed to support Member States in closing persistent digital gaps, improving educational pathways, and ensuring that all citizens can thrive in the digital transition. As emphasised in the **Draghi report** and reaffirmed in the **Competitiveness Compass**, investment in digital skills is essential for revitalising Europe's human capital, fostering innovation, and securing long-term prosperity.

The Union of Skills package[99], adopted on 5 March 2025, reflects the EU's strategic vision for equipping people to succeed in learning, employment, and daily life. It places particular focus on strengthening basic digital skills and building an education and training system that is both resilient and future-proof. As announced in the package, the Commission will propose a 2030 Roadmap on the future of digital education and skills, to promote universal access to digital education for all, alongside the development of an AI literacy framework and support the integration of AI in educational settings. The roadmap will also address online safety, digital well-being, and the role of technology in fostering educational innovation.

Complementing this, the Action Plan on Basic Skills reaffirms the EU's commitment to quality education for all and introduces a Basic Skills Guarantee. The plan recognises digital skills as part of the essential skill set for modern life and includes several key measures to promote inclusion and digital empowerment. As discussed in the following paragraphs, media and digital literacy are identified as key to active and informed citizenship. There is also a growing demand for proficiency in digital collaboration tools and in skills related to cybersecurity, AI, machine learning and big data. The action plan includes mainstreaming digital and basic literacy teaching in initial teacher education; developing guidelines and best practices for assessing digital skills; creating a basic skills toolkit for apprenticeships, including components on digital skills, and promoting quality learning materials on digital skills, literacy and cybersecurity through initiatives such as the EU Code Week, the Better Internet for Kids platform, and the network of national Safer Internet Centres (see 2.3.2). Attracting digital talent from outside the EU is also complementary to these efforts. To this end, the EU Talent

[99] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: The Union of Skills, COM(2025) 90 final.

Pool[100] will facilitate international recruitment between European employers with job vacancies in shortage occupations and the skilled jobseekers from outside the EU.

Building a stronger digital talent pipeline also requires reinforcing the role of science, technology, engineering, and mathematics (STEM) in education policy. By anchoring STEM as a strategic pillar in the EU's education and skills policies, the STEM Education Strategic Plan and its underpinning actions will contribute to foster the development of digital skills as part of the STEM skills across different levels of education and sectors. The Plan promotes the participation of girls and women in STEM studies and careers, strengthens the STEM talent pipeline, from early education to advanced research and lifelong learning, and supports educational innovation by bringing education industry and research closer together. Improving teaching capacity remains essential for integrating digital skills in education systems. Building on the 2023 Council Recommendation on improving the provision of digital skills in education and training, the Commission established a high-level Expert Group on Informatics Education in July 2024. This group supports Member States by addressing key educational challenges in informatics and providing pedagogical guidance for teachers. To ensure a collaborative and practice-based approach, the Commission is also organising workshops with informatics teachers from across Europe. The final guidelines are expected to be published by the end of 2025 in all official EU languages.

Efforts to promote responsible and inclusive use of emerging technologies are being strengthened through the AI Continent Action Plan. Recognising the accelerating influence of artificial intelligence in daily life, the Commission adopted the plan on 9 April 2025. Aligned with the AI Act and the European Declaration of Digital Rights and Principles, the plan outlines actions to support the upskilling and reskilling of professionals in all fields and the wider population in the use of AI. The plan promotes the responsible and inclusive use of AI in both educational and societal contexts, supporting citizens to understand and safely navigate AI-powered technologies[101].

To support access to learning and improve coordination, the EU maintains a centralised platform for digital skills information and training opportunities. The Digital Jobs and Skills Platform[102] is a one-stop-shop connecting users to high-quality resources and learning opportunities, ranging from basic digital skills to advanced specialisations. In 2024, the platform received 285 000 visits and hosted over 15 000 registered stakeholders. It also anchors the Digital Skills and Jobs Coalition, with 25 national coalitions and 22 national portals linked to the platform, offering updates on national initiatives and supporting cooperation across Member States. Furthermore, on 4 July 2024, the winners of the 2024 edition of the European Digital Skills Awards[103] were announced. Out of 267 applications, five outstanding projects were chosen, showcasing innovative approaches to empowering individuals with digital competences, including fostering digital literacy and inclusion.

Ensuring transparency in digital skills assessment is also a priority. The Commission is currently updating the Digital Competence Framework for Citizens (DigComp)[104] to version 3.0. The current DigComp 2.2 already includes more than 250 examples of knowledge, skills, and attitudes across

---

[100] Proposal for a Regulation of the European Parliament and of the Council establishing an EU Talent Pool. COM(2023) 716 final.
[101] AI Continent Action Plan, COM(2025)165.
[102] European Commission, Digital Skills and Jobs platform. Available at: https://digital-skills-jobs.europa.eu
[103] European Digital Skills Awards 2025 : https://digital-skills-jobs.europa.eu/en/european-digital-skills-awards-2025.
[104] See above.

areas such as AI, datafication, teleworking, misinformation and disinformation. To support implementation, the JRC launched a process in 2024 to define indicative learning outcomes for each competence, provide guidance to stakeholders, and help improve the transparency and comparability of certified digital skills across Europe. The updated digital competence framework will be launched at the end of 2025.

Finally, the Commission is investing in lifelong learning systems. As part of its broader evidence-based approach, the Commission published a report in July 2024 examining how Erasmus+ projects funded under the 2018-2021 KA2 calls have contributed to enhancing basic and advanced digital skills in vocational education and training (VET)[105]. The findings and lessons learned from 30 in-depth case studies and an Annex of 100 inspiring good practices cover crucial areas like artificial intelligence, virtual and augmented reality in VET, industry-specific digital skills – for example, in the agriculture, health or logistics sectors. The results confirmed the added value of Erasmus+ in building capacity for digital skills training within initial and continuing VET.

Member State efforts

Best Practice Accelerator: basic digital skills

To advance their 2030 Digital Decade targets, Member States are implementing a broad spectrum of measures to strengthen digital skills across all segments of the population. The BPA has served as a key forum to support this effort, enabling the exchange of national experiences and the identification of common challenges, and fostering peer learning. More than half of the 34 practices submitted through the BPA focus specifically on boosting at least basic digital skills among those most at risk of digital exclusion.

The digital skills cluster, launched under Slovenia's leadership in July 2024, has facilitated structured coordination among Member States, helping scale up successful approaches. Six thematic workshops held over the course of one year supported in-depth discussion of national measures. These discussions were complemented by contributions from the Digital Jobs and Skills Platform, which brought forward more than 20 additional practices from National Coalitions.

The featured practices place a strong emphasis on human-centred, locally anchored delivery models designed to reach underserved groups–such as older adults, rural communities, individuals with low formal education, and disadvantaged youth. Slovenia alone contributed four initiatives: free adult training for over 23 000 people held over three months; the nationwide rollout of Digi Info Points; the Mobile Heroes project, which brings digital classrooms directly to rural seniors; and a youth-focused initiative which supports non-formal training aligned with DigComp 2.2.[106]

Several Member States discussed how public services can act as inclusive training infrastructures. France's Conseillers Numériques programme embedded trained advisors in community spaces, reaching nearly five million individuals. Italy mobilised young people through a Digital Civic Service and built a national support network. Belgium trained over 6 000 civil servants under its

[105] European Commission, ERASMUS+ projects focusing on digital skills and engaging young people in vocational education and training - Analysis of a selection of good practices.
[106] See above.

Connectoo programme, while Austria's Digital Skills Initiative coordinated inclusion and advanced talent development efforts in government.

Other practices showcased how digital competence frameworks and learning platforms can personalise upskilling journeys. Spain's Generation D platform offers more than 1 700 resources linked to a self-assessment tool. Finland introduced a national digital competence framework, funding over 150 local projects with a strong emphasis on early education. Germany's DigitalPakt Alter established over 300 local hubs to support older adults in trusted, low-pressure digital learning environments.

Despite this solid foundation, persistent challenges remain. Most initiatives rely on informal learning, with limited links to formal qualifications or recognised outcomes. Many are pilot projects or depend on short-term funding, and systematic impact assessments are rare. This makes it difficult to evaluate long-term progress or scale efforts sustainably.

Nonetheless, several success factors are evident. Effective practices tend to be embedded in national digital strategies, implemented through cross-sector partnerships, and delivered by trusted actors within communities. These approaches share a commitment to making digital transformation inclusive, helping people not just access services but gain the confidence to participate fully in the digital society.

2.1.2 A highly skilled digital workforce: ICT specialists and advanced digital skills

ICT specialists are at the heart of Europe's digital competitiveness. As the architects of digital transformation, they drive innovation in frontier technologies, enable productivity gains across sectors, and support the development of human-centric digital services. Their expertise is essential for the deployment and maintenance of advanced infrastructure–from next-generation cloud and data systems to AI factories and EuroHPC JU supercomputers–and for delivering secure, efficient, and trusted digital solutions. In an increasingly interconnected environment, they are also critical for safeguarding Europe's digital resilience, particularly in the face of rising cyber threats.

As demand surges for specialists in areas such as **artificial intelligence**, **cybersecurity**, and **semiconductors**, the EU faces the dual challenge of scaling up a technically skilled workforce while ensuring its diversity, adaptability, and long-term sustainability. Addressing persistent shortages and gaps across these high-growth domains, including supporting gender convergence, will be essential not only for meeting the **Digital Decade target of 20 million ICT specialists by 2030** but also for strengthening Europe's industrial capacity, technological leadership, and strategic autonomy in the digital age.

Progress towards the Digital Decade target

Target (same as previous): A digitally skilled population and highly skilled digital professionals, with the aim of achieving gender balance, where (…) (b) at least 20 million ICT specialists are employed within the Union, while promoting the access of women to this field and increasing the number of ICT graduates.

Source: Eurostat – Labour Force Survey.

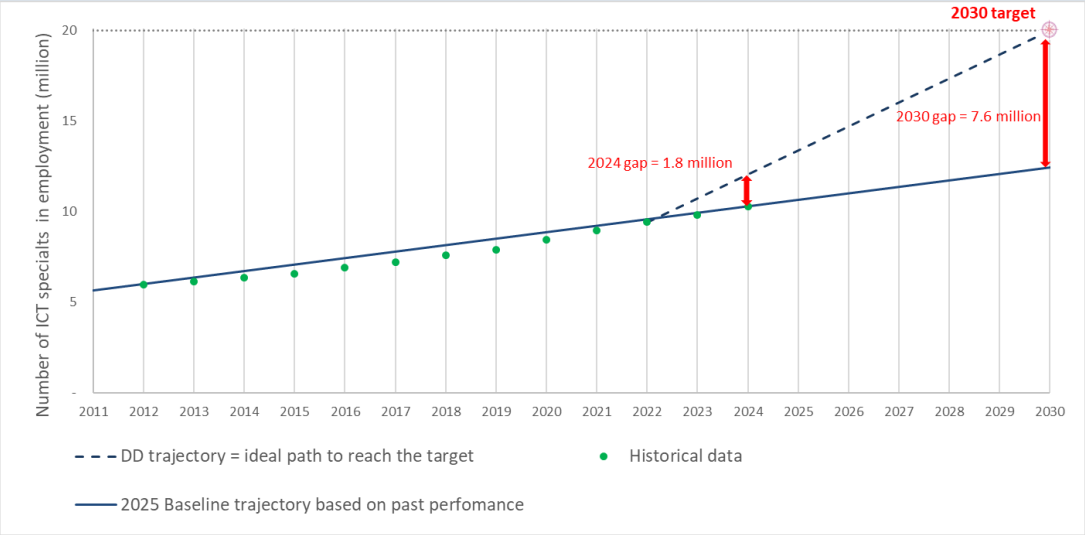
Available data points: from 2011 to 2024.

2024 data values: Number of ICT specialists in employment = 10.3 million (corresponding to 5.0% of total employment); Percentage of women among ICT specialists in employment = 19.5%.

The total number of ICT specialists in employment rose by 471 000, from around 9.8 million in 2023 to 10.3 million in 2024. **This reflects a 4.8% year-on-year growth** in the number of employed ICT specialists. However, ICT specialists still accounted for just 5.0% of total EU employment in 2024, a slight increase from 4.8% in 2023.

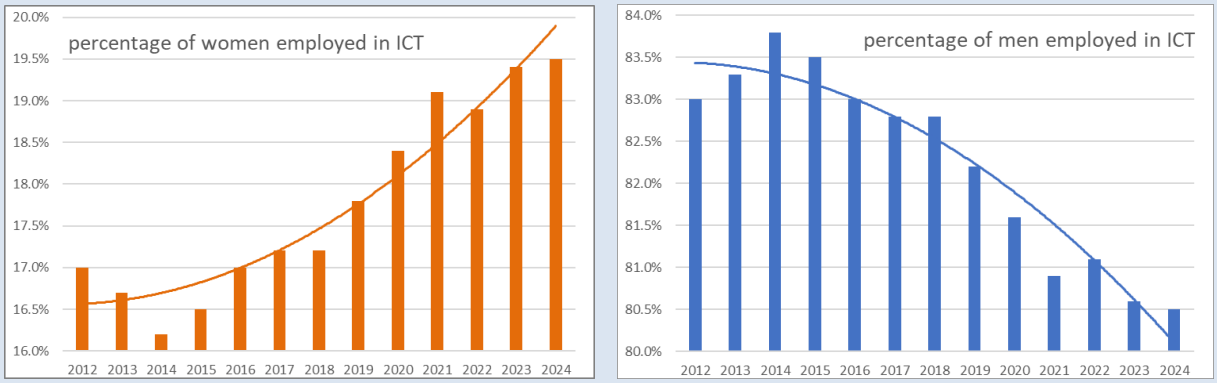
According to the forecast along the baseline trajectory, around 12.4 million ICT specialists are expected to be in employment by 2030, meaning that only **62% of the target will be achieved by 2030** (Figure 29). **In 2024, the value reached by this KPI stood at about 85% of the ideal value along the digital decade trajectory,** around 10.3 instead of 12.1 million. The full target – 20 million of ICT specialists in employment by 2030 - is forecast to be reached only in **2051** if no further actions are taken.

Figure 29: ICT specialists in the EU. Historical data, Digital Decade (DD) trajectory and revised baseline trajectory towards 2030



In 2024, women accounted for 19.5% of employed ICT specialists, a figure virtually unchanged from 2023, when it stood at 19.4%. 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 30). 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 30, left). In contrast, the proportion of men peaked in 2014-2015 and has since declined (Figure 30, right), yet it still exceeds women's representation by more than fourfold.

Figure 30: Percentage of individuals employed in ICT specialists' occupations in the EU by sex (2012-2024). 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. The range of values is different in the two charts.



The EU's data and AI workforce is expanding rapidly, but structural labour shortages are deepening. According to the Data Market Study 2024-2026[107], the number of data professionals in the EU reached 8.23 million[108] in 2024, accounting for 4.5% of total employment and reflecting a growth rate of 4.2% over the previous year. This growth has been primarily driven by the rise of AI and the growing demand for data-driven decision-making across sectors. Yet it has not kept pace with industry needs: the current talent gap stands at 500 000 workers, or 5.7% of overall demand. Projections indicate that this shortfall could reach 631 000 under the baseline scenario and up to 839 000 under a high-growth scenario by 2030, corresponding to 5.8% and 6.8% of workforce demand, respectively. These projections account for expected inflows and outflows in the labour market, including immigration, retirement, sickness, career transitions, and educational output.

Demand for advanced AI competences is accelerating across all sectors of the economy. By 2027, the EU is expected to require between 6.2 and 7 million workers with advanced AI skills[109]. This surge in demand reflects not only the growth of technical roles such as machine learning engineers, AI developers, and prompt engineers, but also the rapid diffusion of AI across non-technical domains[110]. Sectors such as healthcare, manufacturing, finance, and public administration are increasingly reliant on professionals who understand how to manage and apply AI solutions responsibly. Beyond technical expertise, these hybrid roles require cross-disciplinary knowledge to address AI's ethical, legal and organisational dimensions.

AI literacy is becoming essential for a majority of the EU workforce. According to estimates by Cedefop, approximately 61% of workers will need some form of AI-related competence to manage the evolving impact of AI on their jobs[111]. This reflects a shift toward workplace environments where

[107] European Data Market Study 2024-2026

[108] Data professionals are workers who collect, store, manage, and/or analyse, interpret, and visualise data as their primary activity or as a relevant part of their activity. This includes data technicians and data business professionals, but **not users** who, based on sophisticated tools, take decisions after having analysed and interpreted the available data.

[109] LeADS, D1.3 Final ADS demand and forecast report, 2023. Asset/fleet and freight management, claims and fraud management and healthcare are expected to register the highest growth across industries.

[110] Advanced Digital Skills, ADS Demand Dashboard.

[111] Cedefop, Artificial Intelligence in EU Workplaces: another great divide? First insights from Cedefop's AI skills survey, 2024.

understanding algorithmic processes, automation and data ethics is becoming part of everyday professional life–even outside of ICT-specific roles.

Closing the AI skills gap will require a broader and more inclusive talent pool. While it remains difficult to quantify the full scope of the AI skills shortage, the continuous emergence of AI-related tasks and occupations points to a growing and persistent gap. Increasing the participation of women in AI and data professions will be essential for ensuring that the sector can meet future labour demands with a diverse and resilient workforce[112].

As digital threats intensify, the cybersecurity workforce is under growing pressure. Increased exposure to cyber threats and the implementation of new EU regulatory frameworks–including the NIS2 Directive, the Cyber Resilience Act, and the Digital Operational Resilience Act (DORA)–have significantly raised the demand for qualified cybersecurity professionals. In 2024, the estimated need stood at 1.25 million specialists, yet only 951 000 were employed, leaving a gap of 299 000, or 25% of the ideal workforce size. This represents a 9% increase in the gap compared to the previous year[113].

Despite higher investment in cybersecurity, capacity remains constrained. According to the European Union Agency for Cybersecurity (ENISA), EU organisations increased their investments in information security by 1.9 percentage points between 2022 and 2024[114]. However, the share of full-time equivalents (FTEs) allocated to cybersecurity tasks declined–from 11.9% to 11.1% over the past four years–highlighting a persistent shortfall in dedicated staffing despite financial commitments. A flash Eurobarometer survey[115] confirms that over half of companies face recruitment challenges in cybersecurity. The main reasons cited are a lack of qualified candidates (45%) and a shortage of applicants (44%), pointing to structural mismatches in both the quality and quantity of available talent. Many organisations are also forced to rely on non-specialist hires or internal reskilling.

The workforce lacks formal qualifications and remains largely male-dominated. According to the same Eurobarometer survey, among employed cybersecurity professionals, 76% do not hold formal qualifications or certification. A majority of cybersecurity workers (57%) joined the profession by adding cybersecurity skills to an existing role, while 34% were recruited from other professional domains. Gender imbalances are also striking: 56% of companies report having no women in their cybersecurity workforce, despite 70% acknowledging the importance of improving gender balance in the sector.

The EU semiconductor sector is poised for strong growth, but workforce supply is limited. According to the *Skills Strategy 2024* report of the European Chips Skills Academy, the European semiconductor industry employed approximately **382 200 people**[116] in 2023. Of these, around **74% (282 800)** were in core technical roles, while the remainder were in support functions such as

[112] Interface, AI's Missing Link: The Gender Gap in the Talent Pool, 2024.
[113] ISC2, Cybersecurity Workforce Study by ISC2, 2024.
[114] ENISA, NIS Investments 2024 | ENISA.
[115] European Commission, Cyberskills Eurobarometer survey, May 2024.
[116] Around 263 000 were directly involved in semiconductor production. Additionally, approximately 61 000 people worked in companies supplying equipment for semiconductor fabrication, 27 100 in material supply and wafers, 11 340 in developing design software and Intellectual Property, and 19 760 in research and technology organisations.

management and sales. Driven by increased demand and production goals[117] under the EU Chips Act, the sector is expected to grow significantly by 2030.

Semiconductor production expansion will require tens of thousands of new technical professionals. By the end of the decade, projected growth could generate an additional 155 900 new jobs, along with the need to replace around 115 500 existing workers[118]. This creates a combined demand for over 270 000 positions by 2030, largely in technical functions critical to chip design, fabrication, and packaging.

The education system is not producing enough graduates to meet EU semiconductor demand. Despite strong job creation forecasts, the inflow of qualified graduates is expected to increase at a modest pace of just 1% annually[119], constrained by both low enrolment rates and demographic trends. If left unaddressed, this shortfall will result in an estimated talent gap of 75 390 positions in core technical roles by 2030[120], meaning only 64% of projected workforce demand would be met.

Supporting advanced digital skills through EU level initiatives

The EU has introduced targeted policy and funding measures to expand the pool of ICT specialists and improve their skills in critical technology domains. The Competitiveness Compass promotes 'skills and quality jobs' as a key measure to boost Europe's competitiveness by revitalising productivity and investing in skills for leadership in future technologies. While some initiatives - such as the Union of Skills and the AI Continent Action Plan - have already been *outlined in* the context of basic digital skills, this section focuses on how these and other actions are contributing specifically to the development of high-level digital expertise. These measures respond directly to the growing demand for talent in areas such as AI, cybersecurity, semiconductors, and quantum technologies, and form part of a wider strategy to reinforce Europe's technological sovereignty and innovation capacity.

Strengthening Advanced Digital Talent through Strategic Programmes. Building on the broader Union of Skills initiative and responding to the need for a more coordinated approach targeted at emerging skills needs of EU companies, the EU is rolling out a number of flagship measures to support advanced digital skills. Among these is the establishment of four new Digital Skills Academies focused on AI, Quantum, Virtual Worlds, and Semiconductors. These academies aim to complement national education systems by offering specialised training programmes aligned with labour market needs. In parallel, the Commission is promoting joint degrees and the development of future European degrees in digital technologies, with a view to strengthening interdisciplinary skills that are relevant to priority sectors such as biotechnology, health, and climate science.

The launch of the European Advanced Digital Skills Competitions will further encourage excellence and visibility in cutting-edge digital domains among young people across Europe, raising the profile of careers in high-tech domains and fostering excellence in frontier digital fields. The Union of Skills

---

[117] Employment forecasts are estimated based on SEMI's latest forecasts (June 2024) of installed production capacity for the period 2024-2027. Employment elasticity, meaning the percentage change in employment associated with a 1% increase in installed capacity, is estimated using historical employment data from DECISION database and historical installed capacity data from SEMI.

[118] The replacement rate (4%) is calculated using the Cedefop's 'Skills forecast database.

[119] Note that the analysis does not account for non-EU graduates.

[120] 12 500 software engineers, machine learning engineers, data engineers, data analysts and data scientists, 3 800 system designers, 2 400 analogue designers, 3 000 cybersecurity experts, and 54 000 professionals with electrical engineering degrees.

package also includes dedicated training actions under the **Destination Earth (DestinE)** programme, targeting advanced competences in modelling, AI applications, and environmental data systems.

Scaling the AI workforce through the AI Continent Action Plan. Under the AI Continent Action Plan, adopted in April 2025, the EU is increasing its capacity to develop and retain AI talent, particularly in strategic sectors such as industry and public administration. While the Action Plan includes broader actions to promote AI literacy, it also sets out specific measures to strengthen AI skills and talent and enlarge the EU's pool of AI specialists. These include educating and training the next generation of AI experts based in the EU, incentivising European AI talent to stay and to return to the EU and attracting and retaining skilled AI talent from non-EU countries, including researchers.

Expanding the cybersecurity workforce through coordinated EU action. In the field of cybersecurity, the EU has reinforced its response through the Cybersecurity Skills Academy[121], which complements earlier measures focused on citizen awareness and basic competences. Under the Digital Decade Policy Programme, the Academy supports the creation of a European Digital Infrastructure Consortium (EDIC) focused on cybersecurity skills, currently led by Greece. The Commission has also allocated EUR 10 million under the Digital Europe Programme to support the establishment of the Academy[122]. A key deliverable for 2025 is the launch of an industry-academia network, which will connect companies that have pledged to train cybersecurity professionals with higher education institutions, vocational training providers, and university alliances. This network will help scale up the delivery of cybersecurity-specific programmes and expand the pool of qualified professionals in this field.

The Commission is working in parallel with **National Coordination Centres under the European Cybersecurity Competence Centre** to support national implementation. These centres are tasked with building a shared repository of training and certification schemes, identifying relevant funding streams, and establishing indicators to monitor workforce developments at EU level. The Polish Presidency of the Council of the EU has prioritised cybersecurity skills, hosting a dedicated debate under the Horizontal Working Party on cyber-Issues and continuing the momentum generated by initiatives launched during the Hungarian Presidency in cooperation with the Commission and ENISA.

Building semiconductor talent through Chips Competence Centres. To address shortages in the semiconductor workforce, the Industrial Alliance on Processor and Semiconductor Technologies has launched a dedicated Skills Working Group, bringing together industry and stakeholders to coordinate action. In addition, Chips Competence Centres (CCCs) are being established across Member States as part of the EU Chips Act. These centres will play a key role in facilitating collaboration between academia and industry, delivering hands-on technical training, and supporting the development of national and regional talent pipelines.

Preparing Europe's quantum workforce. Under the European Quantum Declaration[123], coordinated quantum competence clusters are being developed to support training, research, and innovation in quantum technologies. These clusters aim to foster collaboration across Member States and help establish a coherent European skills ecosystem in this strategically critical field.

---

[121] Cyber Skills Academy: Get Involved | Digital Skills and Jobs Platform
[122] EU Funding & Tenders Portal
[123] European Commission, European Declaration on Quantum Technologies, 2023.

Fostering innovation, diversity and entrepreneurship through targeted measures. In addition to the above sector-specific efforts, the EU is supporting digital innovation and inclusion through complementary strategic initiatives. The European Data Union Strategy and the EU Start-up and Scale-up Strategy, announced under the Competitiveness Compass, aim to support the development of digital entrepreneurship and ensure that Europe has the skills and data infrastructure needed to compete globally. These initiatives recognise that highly skilled ICT professionals are not only employees but also innovators, start-up founders, and drivers of growth in digital ecosystems.

Promoting greater gender diversity in ICT professions. The Commission has launched the WIDCON (Connecting Women in Tech) project. This initiative seeks to better understand the barriers to women's participation in ICT and create a network of experts and practitioners to identify and disseminate effective solutions. By supporting more inclusive digital talent pipelines, the EU aims to tap into the full potential of its population and build a more resilient, representative, and future-ready digital workforce.

Member State measures

Best Practice Accelerator: ICT specialists

Of the 34 practices submitted under the Digital Skills Cluster, 15 target the ICT specialist workforce, covering diverse areas such as curriculum modernisation, AI readiness, gender equality, and SME upskilling. Several Member States have prioritised reforms to strengthen the education-to-labour transition. In Czechia, informatics and computational thinking have been formally embedded into school curricula, while Finland's National STEM Strategy has reached over 100 000 pupils and 11 000 professionals through teacher training and systemic change e.g. update of education curricula. Austria's Digital Skills Initiative addresses both ends of the skills pipeline, combining awareness-raising with support for ICT apprenticeships and institutional coordination.

A large group of practices focus on building AI literacy and readiness in the public sector. Germany has presented three flagship initiatives: AI Studios, which use participatory workplace training to demystify AI; BeKI, a national advisory centre providing science-based AI guidance to all sectors; and KIPITZ, a platform designed to introduce AI concepts and use cases to civil servants. Similarly, Greece's national training programme for civil servants, implemented together with Microsoft, strengthens public sector capacity in AI, cloud, and cybersecurity through targeted learning modules.

In Ireland, the SuCcES Programme has introduced structural reforms to improve the recruitment and retention of women in academic computing roles, while the INGENIC Network fosters inter-university collaboration on equality measures. TU Dublin's mentoring model supports female students in the early years of study to strengthen belonging and reduce drop-out rates. Croatia's Girls in ICT initiative, which pairs high school students with professional role models through interactive panels and storytelling, has inspired two initiatives in Luxembourg: Girls Deploy Your Digital Talent and Girls in ICT Day, both aimed at motivating teenage girls to explore ICT careers.

At the interface between skills and industry, Romania's Skills in Advanced Technologies for SMEs delivers large-scale upskilling in frontier technologies–AI, RPA, big data, and cloud–to more than 2 000 companies. This business-oriented model responds directly to labour shortages in the private sector while boosting SME resilience and innovation.

Despite these promising efforts, notable thematic gaps remain. To date, no Member State has submitted a BPA practice focused on semiconductor workforce development, vocational ICT

specialisations, or structured cybersecurity career pipelines. While the issue of advanced digital skills shortages was repeatedly raised in workshop discussions, few concrete training programmes or national workforce strategies have been shared in this domain. Similarly, no national AI talent strategy has been presented, nor do current practices include targeted reskilling pathways for mid-career professionals seeking entry into ICT fields.

Challenges also persist with shared dimensions across Member States. Many countries continue to face shortages of qualified instructors and lack well-developed systems for ICT career orientation. Specialisation pathways within formal education are being developed slowly, and efforts to retain women and other underrepresented groups in specialist roles are not yet backed by long-term structures.

Nevertheless, the BPA has helped identify promising dual-track approaches: those that combine mentoring, outreach, and visibility campaigns with systemic reforms in recruitment, training delivery, and public-private partnerships. These initiatives demonstrate that growing the ICT workforce requires not only investing in high-level expertise but also addressing the structural barriers that affect diversity, access, and retention.

To accelerate progress towards the Digital Decade targets, Member States are sharing best practices to build on well tested models, address thematic blind spots, and continue exchanging knowledge and solutions through the BPA platform and its dedicated thematic clusters.

2.2 Deploy digital solutions for people and societies

2.2.1 Digital public services that are user-friendly and accessible to all

Progress towards the Digital Decade targets

Target: The digitalisation of public services, where there is 100% online accessible provision of key public services and, where relevant, it is possible for citizens and businesses in the Union to interact online with public administrations.

KPI definition:

Citizens: Online provision of key public services for citizens, measured as the share of administrative steps that can be done fully online for major life events. The following life events are considered: moving; transport; starting a small claims procedure; family; career; studying; and health.

Businesses: Online provision of key public services for businesses, measured as the share of administrative steps needed to start a business and conduct regular business operations, which can be done fully online.

Source: e-Government benchmark[124].

Available data points: from 2013 to 2024 (break in series in 2020).

2024 data value: Citizens = 82.3 (score 0-100); Businesses = 86.2 (score 0-100).

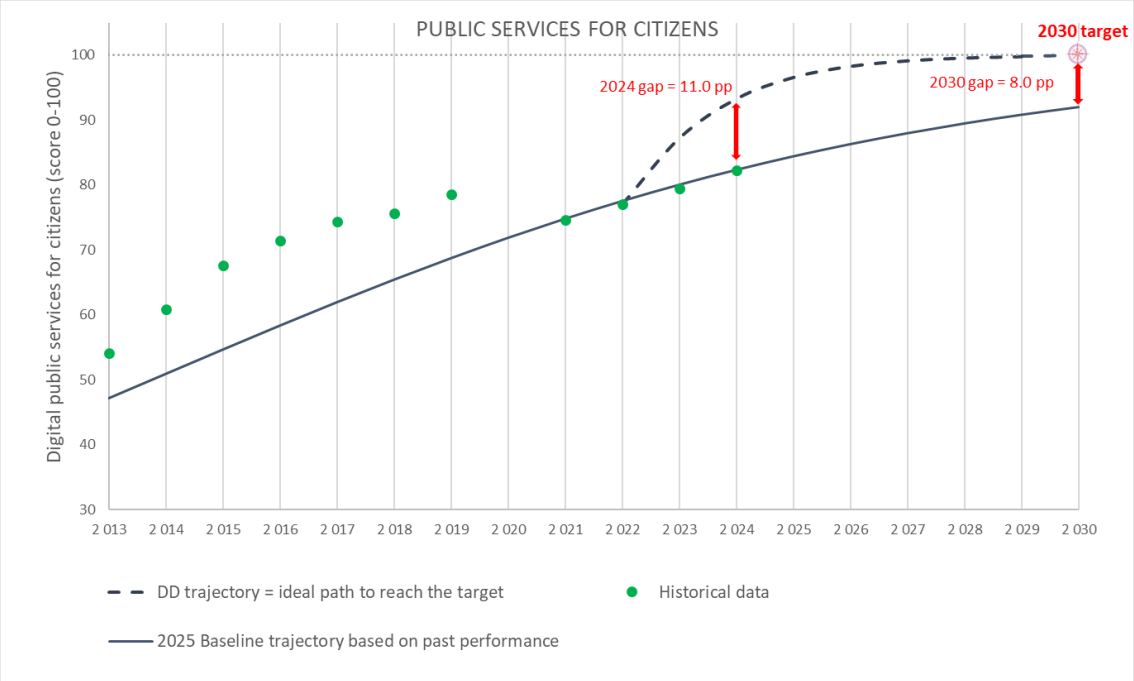
The digital public service score for citizens rose by 2.9 percentage points, from 79.4/100 in 2023 to

[124] eGovernment Benchmark 2025 study. Available at: https://digital-strategy.ec.europa.eu/en/news-redirect/883225

82.3/100 in 2024. This represents a year-on-year increase of 3.6%.

According to the forecast along the baseline trajectory, 92.0% of the target is expected to be achieved by 2030 (Figure 31). In 2024, the score for citizens stood at about 88% of the ideal value along the digital decade trajectory (82.3/100 instead of 93.3/100). However, the full target – a score of 100 corresponding to fully online procedures for all the services – is forecast to be reached only in 2060 if no further actions are taken. The score of cross-border online availability stood at 71.3/100 in 2024, up from 68.4/100 in 2023, +4.2% in one year.

Figure 31. Share of administrative steps that can be taken through online public services for major life events for citizens and resident foreign nationals (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 a mere 0.8 percentage points**, **from 85.4/100 in 2023 to 86.2/100 in 2024**. This represents a year-on-year increase of **only 0.9%**.

According to the forecast along the baseline trajectory, 92.6% of the target is expected to be achieved by 2030 (Figure 32). In 2024, the score for businesses stood at about 91% of the ideal value along the digital decade trajectory (86.2/100 instead of 95.0/100). However, the full target – a score of 100 corresponding to a fully online procedure for all the services – is forecast to be reached not earlier than 2068 if no further actions are taken. The score of cross-border online availability stood at 73.8/100 in 2024, up from 73.1/100 in 2023, approximately +1% in one year.

Figure 32. 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.

Interoperability and enabling legislation

The Interoperable Europe Act, which entered into force in April 2024 and became fully applicable in January 2025, represents a major step in creating seamless digital public services for citizens and businesses across Europe. The Act simplifies and accelerates interactions and data exchanges with public services, helping public administrations in completing the Digital Single Market and reducing administrative burdens, especially for SMEs.

From January 2025 onwards, the Act introduced mandatory **interoperability assessments** for trans-European digital public services, ensuring that cross-border interoperability challenges are addressed early. This new obligation applies both to Member State public administrations and to EU entities. Guidelines for these assessments[125] are available on the Interoperable Europe Portal to guide EU entities and Member States. As part of its digital-ready policymaking framework, the Commission has developed a new **Legislative Financial and Digital Statement** to accompany its proposals. The chapter on the digital dimension includes essential information on the digital aspects of proposals and serves as the Commission's interoperability assessment report, as mandated by the Interoperable Europe Act. It ensures that the Commission thoroughly assesses digital impacts when drafting proposals so that they are fit for the digital age.

The first meeting for the **Interoperable Europe Board,** held on 5 December 2024, marked the operational launch of the Act's governance structure. Comprising high-level representatives from the European Commission and all EU Member States, the Board is developing the 'Interoperable Europe Agenda', a strategic roadmap for interoperability that steers the digital transformation of the EU's public sector. The Board is also responsible for recommending interoperability solutions, which will

[125] European Commission, Guidelines for interoperability assessments, 2024

be labelled as '**Interoperable Europe solutions'**. Since 2024, a new **monitoring mechanism** developed jointly by the European Commission, the JRC and Member States has been in place to monitor the Act's implementation and the state of interoperability in the EU.

The Act also introduces a framework for **interoperability regulatory sandboxes.** These controlled environments allow public administrations and businesses to develop and test innovative digital solutions, generating insights for more consistent, data-driven implementation of EU legislation.

To support the implementation of the Act, the Commission has initiated several support actions. The Coordination and Support Action **Innovative and Connected Public Administrations** under the Digital Europe Programme helps Member States collaborate to identify, develop and test interoperability solutions, paving the way towards a Multi-Country Project on Connected and Innovative Public Administrations. Additionally, the **Interoperable Europe Community**, launched in April 2025, fosters collaboration among stakeholders involved in the digital government and interoperability.

Strategic priorities: technological sovereignty and GovTech innovation

As the EU progresses towards the Digital Decade's goals, the **sovereignty** of Member States over government **digital infrastructures** is becoming crucial. Achieving technological sovereignty requires reducing reliance on non-EU tech providers and improving the ability of the EU to act independently in the digital world. Technological sovereignty allows Member States to drive innovation in the public sector, shape their digital environments – from cloud services to AI solutions – and protect sensitive data. It fosters the development of tailored solutions, actively contributing to the EU's advancements in cutting-edge technologies. Crucially, technological sovereignty allows the EU to pursue an approach to technological innovation that is focused on responsible innovation, ensuring that AI and other emerging technologies align with values such as privacy, fairness, and transparency. This enables Member States to implement secure, sustainable, and citizen-centric digital solutions, reinforcing Europe's vision of a competitive and digitally resilient future.

GovTech plays a key role in the Interoperable Europe Act, combining governance and technology to improve public services and administrative operations. It involves collaboration between the public sector and start-ups and SMEs to procure innovative solutions which streamline administrative processes, foster transparency and improve data-driven decision-making. Notable initiatives under the GovTech umbrella include:

- **GovTech4all Incubator:** A testing arena for public administrations to pilot GovTech solutions in secure environments, fostering experimentation and refining concepts before broader implementation;
- **Public Sector Tech Watch**: An observatory promoting knowledge of emerging technologies within the public sector, serving as a resource hub;
- **The GovTech Connect:** A space for the community of GovTech actors to exchange experiences and seize opportunities.

AI and digital public services

The **use of AI in the public sector** has expanded to include multiple applications such as decision-making and healthcare, increasingly addressing complex challenges and paving the way to significant future advancements. Member States have developed guidelines, strategies, and action plans to ensure that AI benefits are maximised and risks are mitigated. These benefits include automating routine tasks, improving decision-making, and providing personalised services to citizens, all of which enhance public services delivery.

In this context, the European Commission is rolling out the **Apply AI Strategy**, aiming to accelerate AI adoption and innovation in several sectors, including the public sector, by leveraging European-made AI solutions. As part of this effort, under the Digital Europe Programme 2025/2027, the European Commission has allocated a budget of EUR 21 million, to support up to four pilot projects.

Accessibility and simplification

The **Web Accessibility Directive** (WAD) reflects the EU's efforts to ensure digital inclusion and equality. By mandating that websites and mobile applications of the public sector meet certain accessibility standards, the directive plays a crucial role in enabling all Europeans to participate fully in the digital economy and society. The second monitoring period of WAD concluded in 2024. Member States have demonstrated increased commitment to online service accessibility, as evidenced by improved monitoring reports. These efforts include training and awareness-raising activities, ensuring that online services are accessible to all.

In line with the European Commission's goals outlined in the **Competitiveness Compass,** the EU is advancing several interoperability-related initiatives to support simplification and reduce administrative burdens. These measures aim to streamline regulatory reporting for both Member States and EU entities, directly supporting the EU's goal to cut reporting obligations by 25%, with a particular focus on reducing compliance costs for SMEs (on simplification, see chapter 4).

Digital-ready policymaking

Digital-ready policymaking is a priority for the EU, with a view to reducing national implementation costs by optimising expenditure on IT systems required for policy implementation. Collaborative efforts within the European Commission are vital for the effective operation of frameworks such as the **Single Digital Gateway** and the **Once-Only Technical System** (OOTS). These efforts ensure coherent policy implementation and leverage synergies to enhance interoperability across the EU.

The forthcoming European Business Wallet (see below), the Single Digital Gateway, and the OOTS create a cohesive ecosystem of digital solutions that simplify various aspects of life for Europeans.

2.2.2 Trusted solutions for online interaction: the EU Digital Identity Wallet

The **European Digital Identity** (EUDI) Framework supports the EU's digital transformation, the improvement of digital services for people and businesses, and progress towards Digital Decade targets. Central to this initiative is the **European Digital Identity Wallet**, which facilitates the secure storage, management, and validation of personal identification and digital documents. By 2030, the aim is for electronic identification to be accessible for all Union citizens, in line with the Declaration on Digital Rights and Principles.

Digital identity wallets will fundamentally transform EU public infrastructures by providing secure, EU-wide recognised **electronic identification**. These wallets enable online **authentication** for accessing essential services, such as government, healthcare, and banking, thereby eliminating the need for multiple passwords. They also enable the creation of legally binding **e-signatures** and allow for the storage of critical documents like educational credentials, driving licenses, electronic prescriptions and the **European Health Insurance Card**. This functionality ensures easy access and

simplifies daily transactions and travel within Europe, significantly enhancing security, efficiency, and convenience.

2024 was marked by key legislative achievements in the area of digital identity. The **European Digital Identity Framework**[126] came into effect in May, followed by the adoption of nine **implementing acts** in November 2024 and April 2025, setting uniform technical standards and putting in place a robust certification framework. These milestones pave the way for reaching the Digital Decade target mandating that each Member State provides at least one digital identity wallet to every individual and entity by the end of 2026.

Member State measures

In 2024, **Romania** and **Finland** joined other EU Member States in notifying their **electronic identification (eID) schemes**, bringing the percentage of the **EU population**[127] now having access to electronic identification **to 95%**. However, **Hungary**, **Greece**, and **Ireland** have not yet notified their eID schemes. The number of Member States with notified eID schemes has increased significantly, from just one in 2017 to **24 by 2025**–marking major progress towards a more integrated and secure digital public service landscape across Europe.

Member States have taken major steps toward developing and releasing their own wallets by the end of 2026. This will ensure that EU citizens have secure, trusted, and seamless cross-border access to public and private services. Prior to this, Member States only had voluntary mutual recognition of electronic identification schemes.

Four of the implementing regulations set **uniform standards**, **specifications**, and **procedures** for the technical functionalities of the digital wallets, including data formats for the cross-border use of digital documents and measures to ensure their reliability and security. These standards enable Member States to develop secure, privacy-enhancing wallets that are **interoperable** across the European Union. The fifth implementing regulation outlines specifications and procedures for building a robust certification framework for these wallets, guaranteeing their security and the protection of user privacy and personal data.

Digital wallets will bring many direct benefits to EU citizens and residents. Several use cases are already being tested in **Large Scale Pilot (LSP) projects.** The wallets will provide a **digital infrastructure** for a wide range of applications in different public and private sectors. **Students and job seekers**, for instance, can store and share academic credentials for job applications or university admissions. **Drivers** can download, store, and share their driving licences digitally, eliminating the need for a physical copy. **Travelers** can store and share key travel documents, allowing an effortless check-in to flights and hotels.

Pilot projects and stakeholder involvement

Since April 2023, the Commission has funded four **Large Scale Pilot** (LSP) projects to develop and test the EU Digital Identity Wallets across 11 different use cases, involving over 350 entities from nearly all Member States. Building on the valuable insights of these pilots, two new LSPs will launch in 2025, with a combined investment of over 40 million EUR from the Commission and

[126] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, OJ L, 2024/1183.
[127] Based on EU27 population (2023) Demography of Europe – 2024 edition - Interactive publications – Eurostat.

Member States.

New consortia pilots in 2025

Aligned with the Commission's goals to enhance European competitiveness and reduce administrative burdens, the **Wallet Ecosystem for Business & Payment Use cases, Identification, Legal person representation and Data sharing (WE BUILD)** consortium aims to pilot the use of EUDI Wallets across 13 business, supply chain, and payments use cases. This consortium includes more than 170 partners comprising a balanced mix of Member States, public entities, SMEs, large European companies and global leaders in the digital identity ecosystem. The **Advanced Project for Trusted Identity Technologies and Unified Digital Ecosystem (APTITUDE)** will focus on four use cases: payments, mobile vehicle registration certificates, digital travel credentials, and tickets and travel check-in, supported by nearly 120 partners. Both projects are foreseen to run for 24 months starting in Q3 2025, continuing the foundational work initiated by the Commission and building on the knowledge from earlier LSP projects like NOBID, DC4EU, POTENTIAL, and EWC[128].

Funding and investment outlook

The development of EUDI Wallets is supported by funding from the Digital Europe Programme (DEP), which focuses on bringing digital technology to businesses, citizens and public administrations.

With regards to the future investment needs, the testing and development of use cases remain essential for the development of the EUDI Wallets and their features. The goal is to ensure that Member States can offer feature-rich wallets by 2026 and beyond. The LSPs are strengthening this exact process and continue to push the frontier with the new projects starting in 2025 (see above).

As noted in the Competitiveness Compass, digitalisation goes hand in hand with simplification. To better implement EU legislation, companies and public authorities need increased support for capacity building and technical assistance.

The European Business Wallet

Scheduled for proposal by the Commission in Q4 2025, the **European Business Wallet** will serve as a horizontal enabler for Europe's competitiveness. Designed as a core tool to reduce reporting burdens and streamline digital business operations in the EU, the Business Wallet will facilitate secure transactions and open new opportunities for trust service providers. This initiative, building on the European Digital Identity Framework, will create a seamless environment where businesses can interact with public administrations across the EU, and will streamline cross-border regulatory compliance[129].

In 2024, the EU achieved significant legal and practical progress in the development of the EUDI Wallets. With new regulations now in effect, Member States have shown strong commitment to deploy digital public infrastructures and harnessing the benefits of **cross-border interoperability**. Over the next two years, the range of use cases available is expected to continue to expand.

[128] For more information on the LSPs, see SWD 'Monitoring of horizontal recommendations 2024', SWD(2025) 291: https://digital-strategy.ec.europa.eu/en/policies/2025-state-digital-decade-package .

[129] The text is relevant to chapter 4: Coherence and synergy: aligning digital policies and funding at different levels.

2.2.3 e-Health and digital technologies for healthcare

Progress towards the Digital Decade target

Target: The digitalisation of public services, where 100% of Union citizens have access to their electronic health records.

KPI definition: Access to e-health records, measured as: (i) the nationwide availability of online access services for citizens to their electronic health records data (via a patient portal, or a patient mobile app) with additional measures in place that enable certain categories of people (e.g. legal guardians, people with disabilities, older persons) to also access their data, and (ii) the percentage of individuals able to obtain or make use of their own minimum set of health-related data currently stored in public and private electronic health-record (EHR) systems.

Source: Capgemini Invent

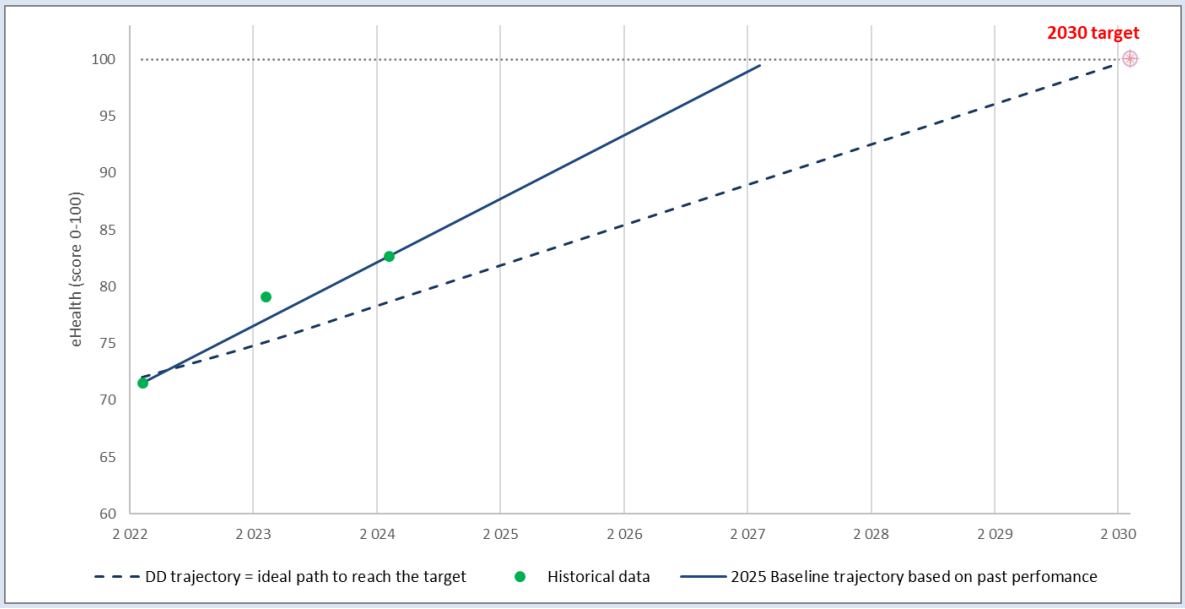
Available data points: from 2022 to 2024

2024 data value: 82.7 (score 0-100)

The access to eHealth indicator rose by 3.6 points, from 79.1 in 2023 to 82.7 in 2024. This represents **a year-on-year increase of 4.5%**.

According to the forecast along the baseline trajectory, **the target is expected to be achieved by the end of 2027** (Figure below).

Figure 33. e-Health composite indicator. Historical data, Digital Decade and revised baseline trajectory.



Member State measures

All Member States have implemented some form of electronic health access, either regionally or nationally, increasing the volume of accessible **health data** and improving access to technologies and opportunities for specific population groups.

Estonia joined **Belgium** in achieving a 100% score in electronic health record access thanks to its new health mobile app. Starting from lower scores in 2023, **Czechia**, **Ireland**, **Romania** and **Slovakia** made

notable progress in 2024, thus narrowing the gap with the leading Member States in the area of electronic health.

Conversely, **Austria** and the **Netherlands** saw their scores decline in 2024, mainly due to discontinued systems and reduced functionalities or availability of services for legal guardians and authorised persons accessing records on behalf of others.

Germany, **Greece**, **Hungary**, **Lithuania**, **Luxembourg** and **Sweden** maintained their previous year's scores. This stability is mainly due to ongoing updates; scores are expected to improve in 2025 and beyond as current efforts come to fruition.

While 2024 saw improvements in the availability **of hospital discharge reports**, no net gains were recorded on medical images. With regard to health data, key improvements were achieved in the handling of personal information; procedures and operations; **eDispensation** information; and lab test results.

The number of healthcare providers integrating data into electronic health records continued to increase across the EU, though a significant disparity persists between public and private sector providers, with the latter lagging behind.

European Health Data Space Regulation

The adoption of the **European Health Data Space Regulation**, effective from 26 March 2025, marks a significant milestone. It ensures that citizens can securely access their electronic health records, both **nationally and across-borders,** improving the efficiency and accessibility of health data for secondary uses such as **research, innovation and policymaking**.

In 2024, a political agreement was reached on the proposed European Health Data Space Regulation, which took effect on 26 March 2025. Efforts to implement the Regulation's requirements are underway.

By March 2027, Member States must publish common specifications for interoperability, security and the logging of electronic health records. Additionally, they need to establish compliance testing environments and cross-border digital health infrastructures (MyHealth@EU and HealthData@EU) and services.

By 2029, Member States must ensure that all priority categories of data (patient summaries, ePrescriptions, lab results) are accessible to citizens for both primary and secondary uses and comply with all other Regulation requirements. Additional data categories such as hospital discharge reports, medical imaging and genomic data must comply by March 2031.

Authentication via a (**pre-)notified eID** compliant with the **eID Regulation** has seen a strong increase across Member States, further supporting **secure and efficient access** to health data.

EU health data infrastructure initiatives

The use of health data and advanced technologies holds great potential to improve citizen access to health services, increase the quality and efficiency of healthcare, foster personalised approaches and support **AI-driven research and innovation**. Stepping up investment and adoption of AI to enhance public services, including healthcare, is a key aspect of the Political Guidelines for 2024-2029[130]. This

[130] European Commission, *Europe's Choice, Political Guidelines for the next European Commission 2024–2029*, 2024.

involves, among other actions, increased investment in frontier technologies, including supercomputing and genomics, while respecting fundamental values and ensuring data protection, privacy and security. In addition, five of the first selected AI factories will include a focus on life sciences and health.

The European Commission's health data infrastructure initiatives contribute to the goals of the **European Health Data Space**[131]**.** For example, under the **European Cancer Imaging Initiative**, launched in December 2022, cancer imaging and clinical data are shared between 12 European countries to support innovation in clinical decision-making and prediction. At the core of this initiative, the DIGITAL-funded **Cancer Image Europe platform** supports data analytics and clinical data access for clinicians, researchers and innovators to develop **AI-based solutions**. A 2024 open call to join the European Cancer Imaging Initiative drew significant interest, underlining its value to the medical imaging community and the broader health ecosystem.

The **1+Million Genome Initiative**, one of the world's largest genomics projects, aims to provide secure access to genomic data and the related clinical data. In 2024, a demonstrator was developed, that showcases how a federated genomic data infrastructure can share data held in different countries, and significant progress was made towards achieving a sustainable legal and business model for the infrastructure. This progress was achieved within the EU-funded implementing projects of the 1+Million Genome Initiative, which will continue guiding the strategic orientation of the initiative and will support preparatory work for the creation of a **European Digital Infrastructure Consortium**, a legal entity, to operate and maintain the European Genomic Data Infrastructure.

The **European Virtual Human Twins Initiative**, launched in December 2023, aims to accelerate personalised care through advanced modelling, with applications in drug discovery, clinical research, and medical training. In 2024, a EUR 24 million procurement launched the development of an advanced platform for Virtual Human Twins. This platform aims to promote interoperability among computational models and datasets, addressing the fragmentation of the VHT ecosystem, particularly by offering high performance computing capacities to smaller innovators and researchers.

In 2024, the Commission launched **two projects under Digital Europe Programme**, allocating EUR 10 million to the development of a cutting-edge federated infrastructure for Intensive Care Unit (ICU) data across Europe. These projects aim to enhance secure cross-border access and interoperability among healthcare datasets.

Cybersecurity in the health sector

In January 2025, the European Commission presented the first of the President's '100 day' initiatives, a European action plan on the cybersecurity of hospitals and healthcare providers. This plan focuses on strengthening the sector's capacities to **prevent, detect and respond** to cybersecurity threats, improve **recovery processes,** and deter cyber threat actors. Specific actions will be rolled out progressively in **2025 and 2026**, in collaboration with health providers, Member States, and the cybersecurity community.

[131] European Commission, European Health Data Space Regulation. Available at: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en

2.3 Protect people, including minors, online

In the last decade, digital services have considerably changed the daily lives of all Europeans, including children and young people, transforming and multiplying the ways they communicate, learn, and express their opinions and ideas. Online platforms have taken a crucial role in shaping daily interactions, whether for commercial, educational, leisure or social purposes. Beyond the opportunities they offer, they also bring challenges, such as the rapid dissemination of illegal and harmful content–including hate speech, terrorist propaganda, unlawful images, and marketing of counterfeit products. The pervasive nature of these platforms necessitates robust regulatory frameworks and a whole-of-society approach to manage their extensive impact, as advocated in the Declaration on Digital Rights and Principles.

2.3.1 Preserve safety, security and wellbeing in digital environments

Across the European Union, online platforms have become an integral part of life. Today, Amazon reaches nearly 2 in 5 Europeans[132], Google Search is used by almost every person in 1 out of 2 households in the EU[133], and YouTube is used by almost every European[134]. Social media platforms also command significant attention, with Instagram and Facebook each catering to around 3 in 5 people in the EU[135]. And platforms like X, Pinterest, and Snap engage about 20-25% of Europeans each[136].

Moreover, EU residents are active online consumers, with **77% of EU internet users having bought or ordered goods or services online in 2024**[137]. They have solid online safety awareness - in 2023 roughly 7 out of 10 (69.6%) individuals undertook at least one action to protect their personal data online[138]. According to the 2024 Special Eurobarometer on Justice, Rights and Values, 72% of respondents across the EU indicated having heard of the GDPR[139].

In the past six months alone, over 10 billion content moderation decisions were made by online platform providers[140], underscoring the colossal volume of information being managed and the growing need for clear and consistent standards.

Fostering online safety and rights protection at EU level

To create a safe, fair, and transparent digital space that upholds user rights and security, the EU has adopted the **Digital Services Act (DSA)**, a landmark legislative act establishing a comprehensive legal

---

[132] Amazon EU Store Transparency Report

[133] Signed-out recipients, versus 356 million signed-in recipients, Google Transparency Report, information about monthly active recipients under the Digital Services Act (EU), https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-24_2024-7-1_2024-12-31_en_v1.pdf.

[134] Ibid, signed-out recipients, versus 459 million signed-in recipients.

[135] For both the Facebook and Instagram numbers are based on the most recent DSA transparency reports of Meta, covering April to September 2024.

[136] The latest transparency report puts X at 106 million users, X transparency: AMARS in the EU; Pinterest's total authenticated user base is 81 million. Pinterest, Digital Services Act; Snap, EU transparency page

[137] Eurostat, (isoc_ec_ib20).

[138] At least one of the following: blocked or limited cookies, checked website security where personal data is provided, limited access to social media profile or shared content, read privacy policy statements, refused use of personal data for advertising, restricted or refused access to geographical location. Eurostat 2023.

[139] European Commission, Special Eurobarometer 552, Justice, rights and values - October 2024 - - Eurobarometer survey.

[140] See data of the DSA transparency database. Available at: https://transparency.dsa.ec.europa.eu/.

framework to address the **inherent risks posed by online platforms and set out the responsibilities** of digital services providers.

The DSA categorises intermediary service providers into different tiers, with more extensive obligations for **Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs)**. These platforms, categorised based on the average number of their monthly users, are required to adhere to stringent compliance rules. In 2024, the EU expanded this list to 25 VLOPs and VLOSEs, most recently including platforms like Shein, Temu, and XNXX. The Commission exercises its enforcement mandate with vigilance, initiating formal proceedings against any suspected non-compliance.

The DSA provides regulators and platforms with a varied set of tools and mechanisms to proactively manage risks. For example, one key obligation for platforms is to implement **'notice and action' mechanisms**, which allow users to report illegal content effectively. Service providers are required to process these notifications in a timely manner, giving priority to those submitted by **trusted flaggers** (independent experts in detecting illegal content).

To uphold the robust standards set by the Digital Services Act, the European Commission actively engages in comprehensive enforcement actions. This involves launching formal proceedings against platforms that are suspected of non-compliance. In 2024, notable cases included actions against major entities like TikTok, Meta's Facebook and Instagram, AliExpress, and Temu. The Commission currently has 13 open proceedings, having **closed its first proceedings, against TikTok, in August 2024** and most recently opened proceedings against four adult content platforms in May 2025. The proceedings are focused on issues such as content transparency, the protection of minors, and dissemination of illegal products.

In addition to launching formal proceedings, the Commission has sent over 100 requests for information (RFIs) to gather critical data from VLOPs and VLOSEs. The RFIs target priority areas, including the spread of illegal content and disinformation, consumer protection, and digital transparency e.g. in advertising.

Collaboration is essential for effectively managing the intricate challenges of digital governance. By endorsing voluntary codes of conduct to counter harmful content and by fostering inter-agency partnerships and coordinated efforts between law enforcement bodies, such as Europol, and Digital Services Coordinators (DSCs) across Member States, the EU unites various stakeholders in a collective mission. These initiatives drive a cohesive response to illegal content and systemic risks, reinforcing a digital ecosystem grounded in mutual responsibility and proactive engagement.

In a collaborative effort to mitigate systemic risks, **in January 2025 the EU endorsed the Code of Conduct on Countering Illegal Hate Speech Online+**. The Code represents a commitment by stakeholders to actively combat harmful content. It strengthens the way online platforms deal with content that EU and national laws define as illegal hate speech through commitments on: terms and conditions; the review time for notices of illegal content; the transparency of content moderation; multi-stakeholder cooperation; and awareness-raising. In this way, the **Code facilitates online platforms' compliance with the DSA** when it comes to risks of dissemination of illegal content through their services.

As digital commerce continues to expand, one of the European Union's priorities has been to create a harmonised framework to ensure fair trading practices and consumer protection across its single market. In February 2025, the **e-Commerce Communication** was adopted to protect consumers and

ensure that products imported via e-commerce comply with EU rules and fair-trading practices[141]. It proposes a comprehensive set of actions across the entire life cycle of the goods[142], **prioritising the enforcement of digital rules, in particular the Digital Services Act, and calls for strengthened cooperation among all relevant authorities in areas such as customs, environmental protection, product safety and consumer protection, while promoting the use of digital tools**. Looking ahead, the Commission plans to closely monitor the implementation of these initiatives and assess their impact on the digital marketplace.

In addition, in the seven years since **the General Data Protection Regulation** became applicable, it has empowered people by allowing them to have control over their data. It has also helped create a level playing field for businesses and provided a cornerstone for the panoply of initiatives that are driving the digital transition in the EU. There has been a significant uptick in enforcement activity by data protection authorities in recent years, including the imposition of substantial fines in landmark cases. Data protection authorities have **imposed over 6 680 fines amounting to around EUR 4.2 billion[143]**. These activities include fines against big tech companies like Meta, Amazon and TikTok.

By November 2025, a comprehensive evaluation will be conducted to determine **how effectively the DSA interacts with other EU rules**, such as data protection and consumer protection legislation, and to identify areas for improvement[144].

Digital Markets Act[145]: Users and businesses have more control over their data

Barriers to data access can lead to less contestability, less innovation and less choice for users. Users can now choose whether they agree for their data to be combined and/or cross-used across the services of 'gatekeepers' (a designation under the DMA for large online platforms offering core platform services). For example, **Alphabet** now gives users the possibility to decide whether their personal data is used and combined, for profiling purposes, across Alphabet products like Search, YouTube, Ad services, Google Play, Chrome, Google Shopping and Google Maps.

All gatekeepers now offer **data portability** solutions for users and enable easier **data access** for businesses. For example, users of **Google Search, Facebook** or **TikTok** can give access to their historic and future data to authorised third parties, to enable these parties to offer competing or innovative services.

2.3.2 Protect children

According to 2025 Digital Decade Eurobarometer, the **vast majority of respondents believe that public authorities need to take urgent actions to: protect children online** from the negative impact of social media on mental health (93%); restrict access to age-inappropriate content through age

[141] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A comprehensive EU toolbox for safe and sustainable e-commerce, COM(2025) 37 final.
[142] European Commission, Factsheet on the e-Commerce communication, February 2025.
[143] Communication from the Commission to the European Parliament and the Council: Second Report on the application of the General Data Protection Regulation, COM(2024) 357 final.
[144] As mandated by Article 91 DSA.
[145] See Chapter 1 of this SWD.

assurance mechanisms (92%); and tackle cyberbullying and online harassment (92%)[146]. Among respondents of the 2024 Youth survey (aged 16-30), **social media is the top source for news on political and social issues**, with 42% relying on it, followed by television with 39%. The preference for TV increases with age, and older respondents in this age group are more likely to use online news platforms and radio[147].

The World Health Organisation's Health Behaviour in School-aged Children (HBSC) study published in 2024 reveals that cyberbullying is a significant problem: 1 in 8 adolescents report that they have cyberbullied others, and 1 in 6 having experienced cyberbullying, with boys slightly more likely to report cyberbullying others[148]. In this context, in 2024 the EU-funded Safer Internet Centres received and handled over 54 000 calls where cyberbullying was the main issue (14% of contacts)[149]. On the other hand, issues related to sexual content or contact (including grooming, the nonconsensual sharing of intimate images, and the online sexual coercion and extortion of children (sextortion)) accounted for 24% of all contacts[150]. Research suggests that intensive use of online social networks correlates with loneliness and emotional distress among young people, while this is largely not the case for instant messaging tools[151].

Data from EU Member States also paints a concerning picture of children spending significant amount of time online[152], and lacking awareness about commercial influencer content. 38% of children between the ages of 6 and 12 in Denmark did not recognise this type of content as advertising. Children also tend to **spend considerable sums of money on in-game purchases**, with 7% of them spending more than EUR 80/month. In Finland, 69% of respondents indicated that they **use social media or play games online for more than three hours a day during weekdays**[153]. As a background, **34% of adolescents surveyed in the HBSC study reported playing digital games daily**, with 22% playing for at least four hours on a gaming day[154]. In Poland, in the fourth quarter of 2024, **every second underage Internet user had contact with erotic content**, spending an average of 10 to 14 minutes a day viewing such content[155].

Consequently, harmful and illegal content, conduct, and contact and consumer risks are frequently present for children online. Often using digital products and services designed for adults, children can

---

[146] The Digital Decade 2025 - special Eurobarometer report: https://digital-strategy.ec.europa.eu/en/news-redirect/883227.

[147] Eurobarometer, Youth survey 2024.

[148] Health Behaviour in School-aged Children (HBSC) international report from the 2021/2022 survey presented in 2024, updated every four years, in collaboration with the WHO Regional Office for Europe. Cosma A et al., A focus on adolescent peer violence and bullying in Europe, central Asia and Canada. Health Behaviour in School-aged Children international report from the 2021/2022 survey. Volume 2.

[149] Better internet for kids – review of year 2024

[150] Ibid.

[151] Joint Research Centre, Cabeza Martínez, B et al., Social Media Use, Loneliness and Emotional Distress Among Young People in Europe (9 January 2025). Ca' Foscari University of Venice, Department of Economics Research Paper Series No 01/2025, Available at SSRN: https://ssrn.com/abstract=5089729. The paper uses a survey sample of people aged 16-35.

[152] The largest share (32%) of the participants in the study use three to four hours, 19% use five to six hours, and as much as 7% use seven to eight hours every day, see Skærmbrug og børn og unges mentale sundhed | Ugeskriftet.dk – (in Danish).

[153] From a survey by the Finnish Mannerheim League for Child Welfare. Respondents ranged from 9-22 years of age, but 83% were 13-17 year olds. They surveyed 3 627 respondents.

[154] WHO 2024 HBSC study, Boniel-Nissim, M et al, Volume 6. A focus on adolescent social media use and gaming in Europe, central Asia and Canada: Health Behaviour in School-aged Children international report from the 2021/2022 survey

[155] Fundacja Instytut Cyfrowego Obywatelstwa, Bigaj, M et al. Children's Internet - Report on monitoring the presence of children and young people on the Internet. March 2025 (in Polish).

be particularly exposed to **misleading and aggressive commercial practices online**. In addition, digital services, from social media to interactive games, can expose children to risks such as unsuitable content, bullying, grooming, child sexual abuse or radicalisation. Seeing explicitly violent, aggressive, or sexual content (such as beheadings and extreme pornography) can desensitise children to such behaviour, normalise violence and affect their mental health and well-being. Although 13 is the minimum age for most social media platforms, **many users are younger, as age-gating is generally ineffective for most digital content and services** at present[156].

As shown above, recent years have seen an escalation in **cyberbullying**. That has a profound impact on healthy relationships among minors, their mental health and trust in the digital environment. Cyberbullying is pervasive and challenging to prevent. Despite the high reported numbers, it is likely that the problem is in fact underreported as children often lack sufficient knowledge on reporting tools or do not trust that there will be an appropriate follow-up to their requests and may decide not to act at all.

Supporting children through EU-level initiatives

The European Union has a comprehensive legislative and policy framework to address these topics, including the Digital Services Act (DSA), the Audiovisual Media Services Directive (AVMSD)[157] and the Better Internet for Kids (BIK+) strategy. In addition, the EU AI Act specifically prohibits AI practices that exploit the vulnerabilities of children[158] . Under the Act, high-risk AI applications must ensure that the mandatory risk management system pays special attention to the impact that the applications may have on minors. The EU co-funded network of Safer Internet Centres (SICs) has been established to provide awareness campaigns, trainings, and resources on online safety, including cyberbullying. In 2024 the network and the BIK platform reached more than 35 million users[159].

As the protection of minors online is a clear priority in the **DSA enforcement**, in 2024, the Commission opened four proceedings related to the protection of minors online: two against TikTok and one each against Instagram and Facebook. As a result, TikTok suspended the task and reward programme, which has been criticised for exacerbating the risk of addiction, in the TikTok Lite app and committed not to roll it out – or any similar programme - in the future in the EU. This commitment has been made legally binding.

The Commission has also sent requests for information to three adult content platforms designated as such under the DSA, asking for more details on the measures they have taken to diligently assess and effectively mitigate against risks related to the protection of minors online, including details related to age assurance mechanisms adopted by these platforms. Based on their responses and other analysis, in May 2025 the Commission opened formal proceedings against Pornhub, Stripchat, XNXX, and XVideos which also focus on the risks for the protection of minors, including those linked to the absence of effective age verification tools.

---

[156] European Parliamentary Research Service, Negreiro M, Online age verification methods for children, February 2023.
[157] In particular the provisions on protecting minors against harmful content (Articles 6a and 28b), in particular the requirement to adopt appropriate measures to that end, including through age verification.
[158] This prohibition became applicable as of 2 February 2025.
[159] SWD 'Monitoring of horizontal recommendations 2024', SWD(2025) 291: https://digital-strategy.ec.europa.eu/en/policies/2025-state-digital-decade-package.

President von der Leyen has also placed great emphasis on protecting the mental well-being of users of social media services. In the 2024-2029 Political Guidelines, the President announced an **EU-wide inquiry into the broader impacts of social media and excessive screen time on mental health and well-being of users, particularly children and adolescents**. This evidence-based inquiry will complement existing research and ensure appropriate policy developments in this area. The aim is to provide practical recommendations for stakeholders, including policymakers, on fostering healthy digital habits and mitigating potential harm to young people's mental well-being.

Additionally, upcoming **guidelines on the protection of minors under Article 28 of the DSA** will assist providers of online platforms accessible to children and young people to ensure a high level of privacy, safety and security for minors using their services. The guidelines will include recommendations in areas such as age assurance, default settings, systems content moderation and child rights impact assessments. The guidelines will be applicable to all sizes of online platforms accessible to minors, except if their providers are micro and small enterprises, and are expected to be adopted in 2025.

The Commission is procuring a **short-term age verification solution**, a 'mini-wallet', to bridge the gap until the EU Digital Identity Wallet is available (by end of 2026). The objective is to develop a **privacy-preserving**[160] **age verification** solution that will be localised and published by Member States or other authorised entities in relevant app stores. The technical specifications for the solution are being prepared with input from Member States and other stakeholders. With a design phase in early 2025 and a development phase in the spring of 2025, the white label application is planned to be released by summer 2025. The application will be highly customisable and modular, and ready for localisation and publishing by Member States.

Moreover, the upcoming evaluation of the AVMSD due by December 2026 will provide an opportunity to assess the added value of the Directive's provisions relating to protection of minors against harmful content and, if appropriate, present proposals for their review. The Political Guidelines also provide for an **action plan against cyberbullying** to address the growing trend of abusive online behaviour. The action plan will ensure a safe online environment for children with targeted initiatives to tackle the issue while promoting digital literacy and supporting awareness-raising efforts. The SICs network will be at the core of the action plan, which will also build on existing good practices of tools and services offered at national level.

Member State efforts

In the context of children protection online, there were several developments at national level. For example, **Ireland** adopted its **Online Safety Code** in October 2024. Around the same time, the French national regulatory authority **Arcom** adopted a technical framework determining the minimum technical requirements that adult content platforms need to integrate in their **age verification systems**.

In 2024, **Greece** launched a comprehensive strategy to protect minors from online dangers, particularly focusing on internet addiction and social media overexposure. The strategy aims to

[160] For importance of a GDPR-compliant age assurance see the statement of the European Data Protection Board from February 2025.

create a safer, more supportive online environment for minors while addressing the psychological impacts of internet addiction.

2.4 Protect information integrity and democracy

Disinformation and foreign information manipulation and interference are serious threats to societies, information integrity online and to the inclusive digital public space protected by the Declaration on Digital Rights and Principles. These phenomena can undermine democratic institutions and processes (such as elections) by preventing people from making informed decisions or discouraging them from voting. They also have the potential to polarise societies by pitting communities against each other. The rise of new technologies has made it possible to spread disinformation and manipulate information on a scale and at a speed never seen before.

2.4.1 Tackle information manipulation

There has been a significant rise in **coordinated inauthentic behaviour** (CIB) on social media in recent years. Networks of fake accounts, bots, and troll farms flood digital platforms with misleading narratives, creating the illusion of grassroots support or public outrage. These manufactured campaigns, often directed by state or non-state actors, distort political discourse, influence elections, and weaken societal trust in legitimate institutions.

The spread of disinformation can come from domestic sources, but often it can be linked to **foreign information manipulation and interference (FIMI)** carried out by hostile foreign actors. FIMI refers specifically to coordinated efforts by foreign (often state-sponsored) entities to manipulate the information environment in target countries. These activities are designed to sow discord, undermine institutions, and shape public opinion to serve strategic geopolitical interests. In the context of the current volatile geopolitical environment, FIMI has become a powerful tool in the hands of unfriendly governments trying to undermine our societies.

At the same time, manipulation **of social media algorithms enable the amplification of disinformation faster than ever before**. Actors seeking to spread falsehoods have learned to exploit recommender systems, hijack trending topics, and game-search engine rankings, making it increasingly difficult for the public to distinguish credible information from deliberate deception.

These tactics fundamentally **disrupt public discourse**, often by creating the illusion of widespread support or opposition where none truly exists. One such method is astroturfing**,** a strategy in which coordinated disinformation campaigns pose as grassroots movements. From fabricated petitions and deceptive online comments to mass-coordinated social media activity, astroturfing distorts public perception, manipulates policy debates, and undermines open dialogue. The result is a manufactured consensus that pressures businesses, policymakers, and the public into adopting positions that may not accurately reflect societal views.

This manipulation of public perception is particularly concerning given how difficult it is for individuals to differentiate between truth and falsehood online. The 2024 OECD Truth Quest Survey assessed individuals' ability to identify false and misleading content online across 21 countries. It examined whether certain types of content are more easily distinguishable as false, the role of content themes in detection, and the impact of AI-generated content labelling. According to the survey, participants correctly identified the veracity of content 60% of the time. True claims were detected less often (56%) than false and misleading content (61%). This means that many individuals struggle with distinguishing true content from false content. In general, almost 50% of the EU

population state that they have seen untrue or doubtful information on internet news sites or social media (the figure being over 70% in the Netherlands, for example)[161].

With the **rise of generative AI**, it is likely that this problem will only grow. These tools allow **nefarious actors to produce disinformation content at high speed and on a large scale**. With rapid improvements in technology, much of this content (whether images, audio, or video) is virtually indistinguishable from real content. These tools are already being used by different influence operations trying to manipulate elections and public opinion in general.

EU's efforts to address online information integrity

As part of the European Union's ongoing efforts to tackle online disinformation, the Commission has introduced a range of policy measures to increase the responsibility of online platforms. These measures are designed to ensure that online platforms take proactive steps to combat the spread of false or misleading information, ensuring a safer and more reliable digital environment for all. In **February 2025 the Commission and the European Board for Digital Services endorsed the integration of the voluntary Code of Practice on Disinformation into the framework of the Digital Services Act** (DSA) under Article 45 of that Act. Its conversion into the Code of Conduct on Disinformation will take effect from 1 July 2025. This integration will allow the Code to become a significant and meaningful benchmark for determining DSA compliance regarding disinformation risks. The Code may be considered as an appropriate risk mitigation measure for signatories who are providers of VLOPs and VLOSEs that adhere to and comply with its commitments. In addition, as part of the DSA enforcement action, the Commission has launched four formal proceedings against the major platforms Meta, TikTok and X, which focus on risk assessment and mitigation in the area of information manipulation.

Aside from the conversion, in 2024 the Commission continued monitoring the implementation of the Code of Practice on Disinformation and worked with signatories to implement their commitments, focusing, in particular, on transparency, accountability and cooperation measures in the context of elections (see section below).

The Commission also continued to support the **European Digital Media Observatory (EDMO)**, which gathers fact checkers, researchers and media literacy specialists to contribute to the fight against disinformation, which is particularly crucial in the context of elections. It ensured that all 14 national and regional EDMO hubs, operational since 2023 with geographical coverage of the whole EU territory, remained fully operational through the refinancing of a set of 8 hubs in 2024. Overall, 14 national and regional EDMO hubs have been operational since 2023, **ensuring EDMO's geographical coverage of all of the EU**. Through dedicated taskforces, the work by EDMO and the hubs has been particularly instrumental in identifying and analysing disinformation on the 2024 European Parliament elections, on Russia's war of aggression against Ukraine and on the Israel-Hamas conflict.

The Commission kept supporting **media literacy** projects to strengthen societal resilience against disinformation. In October, a new call for proposals under the **Creative Europe programme** was launched[162], dedicated to innovative cross-border projects helping to enhance Europeans' media literacy skills and limit the detrimental impact of disinformation. In October, EDMO also launched

[161] Eurostat, 'Evaluating data, information and digital content', isoc_sk_edic_i21, 2023 data.
[162] European Commission, Call for Proposals – Cross-Border Media Literacy projects. Available at: https://digital-strategy.ec.europa.eu/en/funding/call-proposals-cross-border-media-literacy-projects.

Guidelines for effective media literacy initiatives, which aim to increase the effectiveness of media literacy initiatives across Europe.

The Commission also remains actively involved in the development of a series of multidisciplinary **research and innovation** projects, with a budget of EUR 28 million for the 2022-2027 period, which aim to create AI-based tools to detect deepfakes and manipulated content in the form of videos, images and voices.

Significant work is being done to combat disinformation and manipulative behaviour online, while also promoting free speech. However, even more can be done, and a greater effort is needed to combat the challenges linked to disinformation.

2.4.2 Support democratic processes and election integrity

When people are repeatedly exposed to false information, their trust in legitimate sources erodes. This leads to a situation where no one knows what to believe, creating an environment where conspiracy theories and scepticism thrive. As trust in institutions like governments, media, and science declines, democratic processes weaken, and social cohesion suffers[163].

While most Europeans think online social networks allow people to get involved in political affairs, they also believe that information found on them cannot be trusted. Around two thirds agree that online social networks can get people interested in political affairs (67%, no change since autumn 2023) and more than 6 in 10 agree that online social networks are a good way to have your say on political issues (62%, + 1 percentage point since autumn 2023). Over 62% of Europeans now express distrust toward political content on social networks, with particularly high levels of concern in Sweden (83%), Spain (73%), and Finland (69%) (Eurobarometer 2024)[164].

Given the growing scepticism toward digital information sources, editorially responsible **media services, their freedom and pluralism have an even more crucial role in empowering people to make informed choices**. However, their fundamental protection faces a medium risk level in the EU, according to the 2024 Media Pluralism Monitor (MPM) by the Centre for Media Pluralism and Media Freedom[165]. The analysis considered elements such as the existence of effective regulatory safeguards to protect freedom of expression both online and offline, favourable conditions for free and independent journalism and the presence of independent and effective media authorities. In 2024 the average risk score for the Member States was 34%, up by approximately 3 percentage points from the 2023 results. The report identified persisting issues such as a lack of transparency in online platforms' removal of media content and journalists' digital safety.

When it comes to risks linked to market plurality, including transparency of media ownership, plurality of media providers and digital markets, in addition to editorial independence from commercial and owner influence, the 2024 MPM gives a high average risk score of 67% for the Member States, albeit a few decimal points lower than in 2023. The main risks derive from the concentration of media ownership and the concentration in the digital markets, which threaten the pluralism of offer and pluralism of exposure, respectively.

---

[163] A JRC study has identified trust as the key indicator for public institutions communication activities to deal with the increased spread of dis- and misinformation, see Joint Research Centre, Smillie, L. and Scharfbillig, M., Trustworthy Public Communications, Publications Office of the European Union, Luxembourg, 2024, JRC137725.
[164] European Commission, 'Standard Eurobarometer 102 – autumn 2024', report on media use.
[165] Media Pluralism Monitor 2024 – CMPF.

EU-level action to support democracy online

As part of its commitment to protecting and promoting democracy in the European Union, the European Commission has been actively working to address the complex challenges posed by disinformation, online manipulation, and electoral interference (see subsection above).

In addition, digital technologies have been used to make democracies more participatory, inclusive, accountable, and responsive, leading to more social equality, and better decision and policymaking processes. The European Commission's Citizens' Engagement Platform[166] has been instrumental in actively involving citizens in EU policymaking, and in 2024, the platform supported the European Citizens' Panels on Energy Efficiency and Tackling Hatred in Society, gathering stakeholders' ideas to shape relevant policy developments.

In the context of elections, the Commission has taken concrete steps to mitigate systemic risks and ensure the integrity of electoral processes. Beyond the **DSA Guidelines on the Mitigation of Systemic Risks for Electoral Processes** from spring 2024, throughout 2024 and into 2025, the Commission has closely monitored and supported elections across the EU, including the European elections in June 2024, sharing expertise with national authorities, organising round tables with stakeholders, and **conducting stress tests to simulate election manipulation and interference scenarios**. To further support Member States' regulators in their work with VLOPs and VLOSEs, the Commission published a **DSA election toolkit in February 2025**[167]**,** summarising best practices and approaches to mitigating risks such as hate speech, online harassment, and manipulation of public opinion.

In December 2024, the Commission took a significant step by opening formal proceeding against TikTok under Digital Services Act, as response to the 2024 Romanian presidential elections. This decision followed indications of foreign interference in the elections, with the Commission suspecting that TikTok may have failed to properly assess and mitigate systemic risks to election integrity. The investigation focuses on TikTok's management of risks related to its recommender systems and policies on political advertisements, paying particular attention to whether the platform has diligently addressed regional and linguistic aspects of national elections.

Important work has been done with signatories to the **Code of Practice on Disinformation**, which has led to the successful implementation of the **Rapid Response System (RRS)** ahead of the European Elections. The RRS enabled fact checkers and civil society organisations to flag suspicious content and receive feedback from platforms, helping to protect the integrity of the electoral process. The Code's taskforce has also delivered new measurements of structural indicators, providing insights into online disinformation trends during the electoral period. Besides the European Parliament elections, the **Code's RRS was activated for the elections in France and Romania in 2024 and continues to be applied in 2025.**

In regular public reporting on the implementation of their commitments under the Code, signatories provided dedicated information on the election-specific actions they had implemented for the European elections (as well as Russia's war of aggression against Ukraine and the Hamas terrorist

[166] European Commission, Citizens Engagement Platform, available at: https://citizens.ec.europa.eu/index_en.
[167] European Commission, Commission presents new best-practice election toolkit on the Digital Services Act, Press Release, 20 February 2025.

attacks on Israel)[168]. The Code's taskforce also delivered new measurements of the Code's Structural Indicators, giving insights into online disinformation covering the electoral period across major online platforms in the EU.

In addition to these initiatives, the Commission has been supporting the work of the **European Digital Media Observatory** (EDMO), which monitored the EU-wide online information space and exposed disinformation during the 2024 European Parliament elections[169]

A comprehensive toolbox employed by the Commission on the nexus of election integrity and information manipulation includes also the recommendation on inclusive and resilient electoral processes which encourages measures to protect the information environment around elections [170]. It recommends developing public awareness, media literacy and critical thinking to address information manipulation, interference and disinformation related to elections Additionally, the Commission supports Member States through the **European Cooperation Network on Elections**, which fosters dialogue, cooperation and practical solutions to a range of threats in the context of elections, including FIMI and disinformation. In 2024, the rules on **transparency and targeting of political advertising** were introduced[171]. Among others, they tackle the use of advanced targeting techniques and the threat of information manipulation and interference.

Looking ahead, the Commission is committed to stepping up its efforts to counter foreign information manipulation and interference online, as outlined with the **European Democracy Shield** initiative[172], announced in the 2024-2029 Political Guidelines. This initiative aims to enhance Europe's capacity to detect, analyse, and proactively counter disinformation and information manipulation building on the work already done under the **European Democracy Action Plan and the Defence of Democracy Package**. The Commission further plans to bolster fact-checking coverage across Europe through a **European Network of Fact Checkers**, which will play a critical role in detecting and countering disinformation. In addition, the Commission will reflect on ways to continue supporting independent and pluralistic news media and a trustworthy information sphere.

The Commission's actions demonstrate a comprehensive and multifaceted approach to supporting information integrity in the EU, including in the context of democratic processes. By combining regulatory frameworks, stakeholder and citizen engagement, and support for fact-checking and media literacy initiatives, the Commission is working to create a more resilient and transparent online environment, where citizens can access accurate and trustworthy information.

---

[168] Available at : www.disinfocode.eu.

[169] For details, see the Commission's Report on the 2024 elections to the European Parliament (publication pending at the time of writing).

[170] Commission Recommendation (EU) 2023/2829 of 12 December 2023 on inclusive and resilient electoral processes.

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

[172] See the Commission's call for evidence for the European Democracy Shield.

3 Harnessing digitalisation for the green transition

The green and digital transitions are at the heart of the **Competitiveness Compass for the EU**[173] to regain competitiveness and secure sustainable prosperity. The Compass identifies high and volatile energy prices as a key challenge and sets out areas for intervention to facilitate access to clean and affordable energy. In this context, digitisation is **a key enabler to maximise the synergies between the green transition and competitiveness**, e.g. by reducing costs, meeting resource needs, optimising supply chains, enabling circular scalable business models. Digitalisation, when properly used and governed, is also a catalyst for a green, inclusive and competitive economy due to its net positive impact on the environment and climate. By ensuring that the environmental benefits of digitalisation outweigh its negative impacts, the EU will be able to meet the sustainability targets and objectives already set, in particular as part of the **European Green Deal**[174]. Policy priorities and key performance indicators should concentrate on quantifying and amplifying the net environmental impact of digitalisation. In this way we will boost green innovation and deliver measurable energy and material efficiency gains, making the EU more competitive as an economy and less dependent on materials and resources.

To complete this holistic approach as highlighted in the report on **'The future of EU Competitiveness'**[175], the green/digital twin transition must bolster economic vitality without compromising growth, innovation and social equity, emphasising that Europe's future lies in harmonising environmental objectives with economic and social policies. The Political Guidelines 2024-2029[176] task the new Commission with resolving the inherent conflicts and maximise the synergies between economic competitiveness and environmental sustainability, recognising the key role of digitalisation in the endeavour. This is also reflected in the mandate of the Executive Vice-President for *Technological Sovereignty, Security and Democracy*[177]. It emphasises leveraging digital innovation to drive the green/digital twin transition, ensuring Europe's competitiveness while fostering a climate-neutral, resource-efficient, and socially inclusive future, including sustainability as a goal for the review of the Digital Decade Policy Programme.

The Digital Decade sets the objectives of ensuring not only that digital infrastructure and technologies become more sustainable and resource-efficient but also that digital infrastructures and solutions deliver benefits across all three dimensions of sustainability: economic, social and environmental. This chapter focuses on the environmental benefits and includes several references to the sustainability of infrastructure targets, in particular edge nodes and semiconductors. It also points to ways of maximising the environmental and climate benefits of digitalisation. In summary, the Digital Decade's objectives and targets, like the European Declaration on Digital Rights and Principles, are all seeking to promote sustainable digital technologies, products and services with a minimum negative impact on the environment and society. We need to continue developing and

[173] Competitiveness Compass for the EU, COM(2025) 30 final.
[174] European Commission, 'The European Green Deal', 2020.
[175] Draghi, M., 'The future of European competitiveness', 2024.
[176] European Commission, Political Guidelines for the next European Commission, 2024.
[177] European Commission, Henna Virkkunen – Mission Letter, 2024.

utilising science-based methods to measure and better understand the environmental impact of digitalisation and to provide accurate and easy-to-understand information on that impact in a transparent and open way. This includes, in particular, energy and material consumption of digitalisation as well as positive effects (e.g. avoided emissions) and negative indirect effects (e.g. rebound).

3.1 Key trends and prospects

The digital transition aims to minimise conflicts and maximise synergies between the green transition and the competitiveness of EU industry. Digital technologies present opportunities for streamlining operations and improving resource efficiency, which can help reduce the costs associated with the green transition. Automation and data analytics, for example, can optimise energy consumption and waste management. Additionally, digital solutions can simplify compliance with environmental regulations by automating emissions tracking and reporting, making it easier for businesses to meet standards while avoiding high costs. Advanced technologies like blockchain and IoT can also enhance supply chain transparency and efficiency, helping companies mitigate disruptions and transition to sustainable materials more effectively. Furthermore, digital tools enable businesses to assess risks linked to green investments by providing predictive analytics and scenario modelling, facilitating informed decision-making.

To maximise synergies, digital technologies foster innovation, enabling companies to develop sustainable products and services quickly and efficiently. Collaborative platforms can also drive partnerships in research and development (R&D) for green technologies. The availability of real-time data allows businesses to align sustainability goals with strategic objectives, improving overall competitiveness. Digital tools also enhance customer engagement by helping companies communicate their sustainable practices more effectively, thus increasing brand loyalty and market reach. Platforms for training and skill development ensure that employees gain the expertise needed to support both digital and green transitions, preparing the workforce for the future[178]. Moreover, digital technologies enable the integration of circular economy practices by tracking product life cycles, which allows companies to design for reuse and recycling, further boosting competitiveness. Finally, scalability is another advantage, as digital solutions help businesses implement green initiatives more efficiently across various operations and geographies.

The green transition also presents several opportunities for ICT enterprises in the EU. The demand for energy-efficient technologies opens doors for innovation, such as the development of low-power processors, AI-powered energy management systems, and green cloud solutions. These innovations not only meet environmental needs but also create new business models. ICT companies can also benefit from adopting energy-efficient infrastructure, like renewable energy-powered data centres with advanced cooling systems, which reduce both emissions and long-term energy costs. Additionally, the growing emphasis on sustainability creates new market opportunities for green ICT solutions, including software and hardware for environmental monitoring and smart grids. Digital tools, such as IoT solutions and blockchain, are pivotal in supporting sustainability by optimising resource usage and ensuring sustainable supply chains. The transition to a circular economy offers ICT companies the chance to lead in developing recyclable, repairable, and modular products,

[178] IEA, World Energy Employment 2024, 2024.

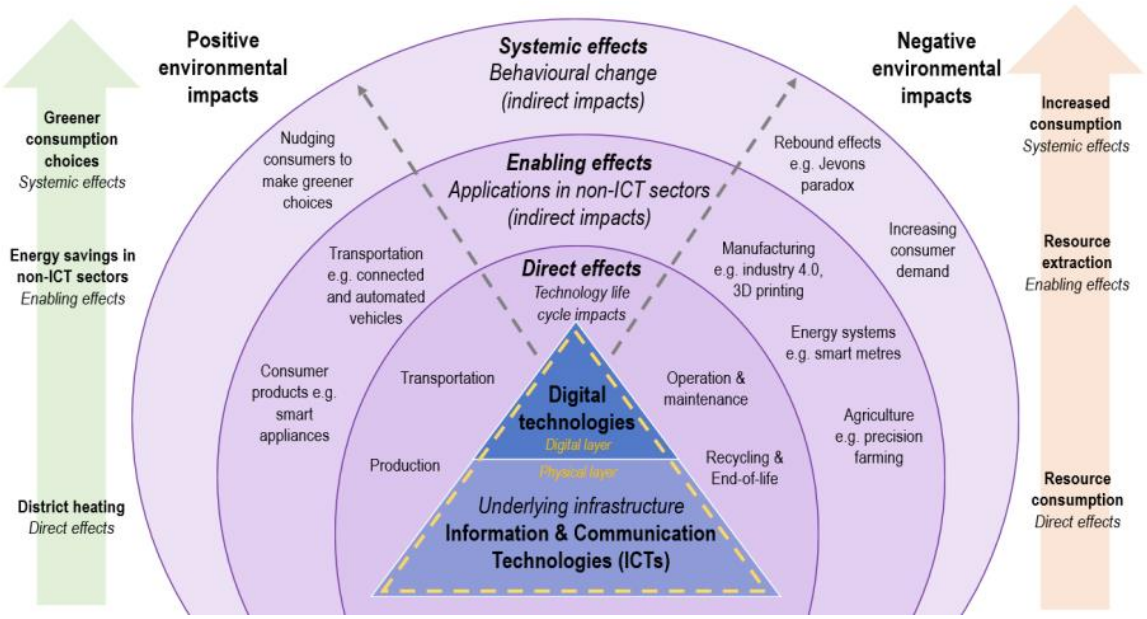
differentiating themselves in the market and appealing to eco-conscious consumers. Furthermore, when the net impact of digital solutions is positive, **ICT companies can tap into green financing for the development and deployment of digital solutions provided by the EU**, such as the European Green Deal Investment Plan and Horizon Europe funding, to support their sustainability efforts.

Regarding the key trends we can identify worldwide, **the ICT sector keeps growing significantly, reflecting the global increase in digital adoption**. The number of internet users worldwide grew by 160%[179], and broadband networks were substantially expanded. This expansion in digital connectivity supports work, learning, and economic activities but also raises concerns about the environmental effects of ICT proliferation. While digital technologies enable improvements in energy efficiency and agriculture, the overall environmental impact is still under scrutiny. The growth of the ICT sector has been rapid, outpacing overall economic growth. Technological advances, such as the miniaturisation of processors and increased storage capacity, have driven this growth, but it is unclear whether these efficiency gains have led to a net positive environmental impact. Large tech companies have become major consumers of renewable energy and their demand for electricity can strain delivery of renewable resources to smaller firms or other sectors of the economy such as the electrification of mobility. Four large ICT companies are among the world's top 20 corporate electricity consumers[180]. Power purchase agreements (PPAs) have helped stabilise the renewable energy market, though they do not always guarantee consistent low-carbon electricity consumption. Transparency regarding the carbon intensity of digital technologies' energy use is crucial for understanding their true environmental impact.

The environmental impacts of digital technologies vary across three distinct categories: direct, enabling, and systemic effects. While these technologies contribute to more efficient practices and sustainability in some areas, they also present significant challenges related to resource consumption, waste, and emissions. Understanding these categories helps distinguish the different ways digital technologies influence the complexity of their environmental impact.

[179] ITU, World Telecommunication/ICT Indicators Database, 2023.
[180] The World Bank & ITU, Measuring the Emissions & Energy Footprint of the ICT Sector, 2024

Figure 34. Digital technologies can have direct, enabling, and systemic effects on the environment, with positive and negative impacts (source: OECD, 2024)



The '**direct effects**' of digital technologies refers to their immediate impact on the environment through resource consumption and emissions. For example, data centres generate significant amounts of excess heat, which could be repurposed for district heating or local energy networks, although scaling up such solutions remains challenging. Similarly, wastewater from data centres can be cleaner than the source water, but its treatment still requires energy and generates emissions. Data centres waste over 90% of the energy they consume as heat[181], which could potentially be used to decarbonise nearby buildings. However, while centralisation has led to energy efficiency gains in large operations, the overall energy demand continues to rise. The direct ICT sector footprint is the subject of many studies with various definitions of 'ICT sector' and different methodologies. As a result, **estimates of the ICT sector footprint vary widely from 1.7% to 4% of global greenhouse gas (GHG) emissions**. The ICT sector's electricity demand is projected to triple by 2030, necessitating urgent action on green energy procurement and efficiency standards. Regarding the sectoral breakdown, mobile networks would contribute 68% of telecommunications emissions while fixed networks would contribute around 24% and data centres around only 8%[182]. Consumer devices and cloud services also contribute significantly. Additionally, the environmental impact of digital technologies extends to the mining of critical materials like cobalt and lithium, which raises significant environmental and human rights concerns. Digital technologies also contribute to e-waste, which is often improperly disposed of in developing countries, exacerbating environmental harm. Despite regulations such as the EU's WEEE Directive, recycling rates for e-waste remain low. The increasing energy demands of AI and machine learning systems also highlight the direct environmental effects, with specialised hardware like GPUs being more energy-efficient but still adding strain to energy grids. The AI models require vast computing power, leading to increased use not only of electricity but also of water for powering and cooling data centres. Similarly,

[181] OECD, 'Review of relevance of the OECD Recommendation on ICTs and the Environment', 2024.
[182] The World Bank & ITU, Measuring the Emissions & Energy Footprint of the ICT Sector, 2024.

semiconductor manufacturing relies on the consumption of much water and the use of many rare materials, raising concerns about resource scarcity and its impact on EU sovereignty.

The '**enabling effects**' describes how digital technologies can support sustainability across various sectors by improving efficiency and reducing waste. Recent studies suggest that digital technologies can reduce emissions up to 20% by 2050[183]. High-digital-intensive sectors, for instance, have seen stable or even low growth in greenhouse gas emissions since 2010, showing how digital innovations can help reduce environmental footprints. Digital technologies enable better energy management, such as through AI-driven digital twins, smart sensors, and virtual meeting platforms that reduce the need for travel. In agriculture, digital tools like AI and IoT technologies help optimise resource use, increasing crop yields while minimising water and energy consumption. For example, smart irrigation systems can reduce water usage by up to 30%, addressing water scarcity while maintaining a healthy crop[184]. Similarly, IoT technologies can enable remote repairs, extending the lifespan of products and thus reducing e-waste. In the energy sector, digital technologies support the integration of renewable energy and the management of decentralised grids. Smart grids, energy storage systems, and AI-driven solutions optimise energy flows, reduce waste, and lower reliance on fossil fuels. The installation of nearly 1.1 billion smart meters worldwide in 2021 illustrates how digital infrastructure is already helping create more sustainable energy systems[185]. Smart meters are estimated to save around 3.34% of electricity consumption in private households while at the same time increasing consumers' awareness of energy consumption.

The '**systemic effects**' refers to how digital technologies influence human behaviour and societal patterns toward more sustainable practices. Digital technologies have the potential to nudge individuals and organisation toward greener choices. For example, notifications about energy use or suggestions for eco-friendly alternatives can encourage consumers to reduce energy consumption or make more sustainable purchases. Household spending, which accounts for a significant portion of GDP in many countries, could be influenced by these 'digital nudges', thereby contributing to a broader green transition. The rise of teleworking, facilitated by digital tools during the COVID-19 pandemic, highlights how digital technologies can reduce the need for physical services and travel. However, these technologies also have unintended consequences. Efficiency gains may be offset by 'rebound effects,' where the increased convenience or use of energy-efficient technologies leads to higher resource consumption. For example, purchasing an energy-efficient appliance may result in more frequent use, negating the expected energy savings. Similarly, AI systems may unintentionally encourage emissions-heavy activities, such as greater resource consumption or inefficiencies in autonomous vehicles. To mitigate these effects, the concept of 'digital sobriety' has been proposed, advocating for the responsible deployment of digital technologies that align with sustainability goals. Insights into consumer behaviour, such as addressing biases, can help shape policies like eco-labelling or mandatory information disclosure, further promoting greener choices.

---

[183] The World Economic Forum, 'Digital technologies can cut global emissions by 20%. Here's how', 2022.
[184] Kalpana, Ponugoti & Smitha, L. & Madhavi, Dasari & Nabi, Shaik & Kalpana, G. & Kodati, Sarangam, 'A Smart Irrigation System Using the IoT and Advanced Machine Learning Model: A Systematic Literature Review', International Journal of Computational and Experimental Science and Engineering, 2024.
[185] Behavioural Insights Team of the UK Government, 'Reviewing energy supplier evidence on impacts of smart metering on domestic energy consumption', 2023.

3.2 Addressing the environmental footprint of digitalisation

3.2.1 Data centres, cloud and edge computing, AI

Previous projections regarding the direct environmental footprint of digitalisation are no longer valid due to the latest developments in Generative AI and the resulting stark increase in energy consumption, GHG emissions and water use.

The rapid expansion of digital infrastructure, including data centres, AI computing, cloud services, and telecommunications networks, has significant environmental implications. **Data centres** are major consumers of energy and water. The distribution of energy use within the ICT landscape is shifting. Traditionally dominated by consumer devices, consumption is increasingly concentrated in networks and data centres. This change is fuelled by technological developments such as edge computing, which is projected to represent 12% of the EU's total data centre energy use by 2025 and up to 40% of server capacity by 2030[186.] At the current rate of adoption, Europe's data centre power consumption is expected to almost triple from about 62 terawatt-hours (TWh) today to more than 150 TWh by the end of the decade[187]. Globally, data centres are using 400 TWh; the study's prognosis is that by 2035 this will triple to 1 200 TWh. Therefore, it is crucial to consider the energy source. A big portion of this projected increase is attributed to AI[188]. Relevant studies converge towards an average growth rate in annual data centre energy consumption of 13% per year between 2023 and 2030 (a total increase of 85 TWh)[189]. That is twice the growth rate experienced between 2018 and 2023. Comparatively high energy prices negatively affect the competitiveness of data centres located in Europe compared to other regions of the world. Some cooling technologies mean that a 1 MW data centre can use up to 15.5 million litres of water annually[190]. The limited availability of (renewable) energy and water, especially in regions with a strong data centre presence, in conjunction with high operational costs due to high energy costs in Europe, is a key bottleneck for data centre deployment and results in winner-takes-all scenarios where large cloud service providers pre-empt the purchase of resources in a given region[191]. Technological innovation promises significant resource savings and – by extension – lower operating costs. For example, innovative forms of cooling can significantly reduce water and energy consumption. Adopting highly sustainable technologies can give data centre operators a competitive edge and help them overcome bottlenecks related to resource scarcity. At the same time, under the right conditions, data centres can make a positive societal contribution by offering flexibility services to the grid and supplying nearby areas with waste heat.

The recast EU Energy Efficiency Directive requires large data centres (with more than 500 kW of installed capacity) to report on a number of KPIs that inform on the environmental impact of data centres. In March 2024, the Commission adopted Delegated Regulation (EU) 2024/1364 laying down the key performance indicators which data centre operators must report to a European database by

---

[186] European Commission, 'Energy-efficient Cloud Computing Technologies and Policies for an Eco-friendly Cloud Market', 2020.
[187] McKinsey, 'The role of power in unlocking the European AI revolution', 2024.
[188] IEA, 'Energy and AI', 2025.
[189] McKinsey, The role of power in unlocking the European AI revolution, 2024. ; IEA, 'Energy and AI', 2025.
[190] The World Economic Forum, 'Circular water solutions key to sustainable data centres', 2024.
[191] These are scenarios in which a large data centre operator buys up available resources and thus prevents others from entering the market in a specific location.

15 September 2024 pursuant to Article 12 of the Energy Efficiency Directive. These cover detailed information regarding the energy and water consumption, cooling efficiency, use of waste heat etc. The data collected will inform further policy action under the Energy Efficiency Directive. The KPIs defined in the Delegated Regulation will form the basis for an EU-wide rating scheme for data centre sustainability, work on which is taking place over the course of 2025. The first annual reporting yielded incomplete information on data centre sustainability performance in the EU, but it was nonetheless a significant step forward in establishing the reporting and the respective platform. The second reporting cycle has a deadline of 15 May 2025. Member States are encouraged to work with their respective national industries to improve the data collection, considering the importance of adequate information for future policy choices. The Commission will assess the 2024 data available and submit a report to the European Parliament and the Council, exploring further possible policy action such as minimum performance standards for new data centres, in accordance with Article 12(5) of the EED recast.

The future **Cloud and AI Development Act** will provide a significant boost to research and innovation in technological solutions that improve data centre energy efficiency and maximise the societal contribution of those solutions. Moreover, the Act will improve the conditions for deploying highly sustainable data centres in the EU and provide incentives for private-sector investments in sustainable data centres, in particular by offering a simplified pathway to deployment as well as other support measures to operators planning innovative and sustainable data centres. The large-scale deployment of data centres will put a strain on the EU's energy grid. The strategic roadmap for digitalisation and AI in the energy sector will propose further measures to facilitate the sustainable integration of data centres into the energy system.

Regarding **water consumption**, many of the data centres which power AI and cloud computing use water-cooled systems, which can consume significant amounts of water.[192] As a policy response to this issue, the aforementioned reporting on data centre sustainability also covers a data centre's total water input, total potable water input, and Water Usage Effectiveness (WUE). These KPIs will also feature in the future rating scheme for data centre sustainability. In addition, the future Cloud and AI Development Act will boost research in water-efficient data centre solutions and consider water usage as a determining factor for whether a planned data centre may obtain access to the benefits that intend to boost the deployment of sustainable data centres in the EU. Moreover, the EU is exploring and promoting alternative more water-efficient cooling solutions, notably in the context of the Water Resilience Strategy. The EU Circular Economy Action Plan[193] promotes water-efficient cooling technologies and encourages reusing excess heat from data centres.

The Clean Industrial Deal and the **Affordable Energy Action Plan**, like the Draghi report, highlight the enabling role of digitalisation and AI in accelerating the EU's energy transition and boosting competitiveness. The upcoming **Strategic Roadmap on digitalisation and AI in the energy sector** will aim to use the potential of digital and AI technologies in energy to accelerate the twin green and digital transitions. **The Net-Zero Industry Act** aims to boost the manufacturing of technologies to digitalise the grids and energy system-related energy-efficient technologies.

---

[192] The World Economic Forum, 'Circular water solutions key to sustainable data centres', 2024.
[193] European Commission, 'Circular economy action plan', 2020.

Concerning **material consumption**, critical raw materials are at the heart of the semiconductors industry, with the production of chips and digital hardware at the centre. Such production depends on rare earth elements (REEs) and metals such as cobalt, lithium, and gallium, which are subject to geopolitical supply risks. The huge development of digital technologies is bringing the fastest growth in the demand for transition minerals. To meet the growing demand for low-carbon technologies, production of minerals such as graphite, lithium and cobalt could increase by nearly 500 per cent by 2050[194]. The EU Chips Act aims to increase European semiconductor production to reduce reliance on foreign supply chains.

e-Waste growth

The ICT sector generates 53.6 million tonnes of e-waste per year globally[195], of which only 17% is properly recycled. Short Lifespan of Devices: Many consumer devices (smartphones, laptops) have limited repairability, increasing premature disposal. The Right to Repair Directive strengthens consumer rights to extend device lifetimes and increase refurbishment rates. The **Ecodesign for Sustainable Products Regulation (ESPR)** introduces mandatory circularity requirements for digital devices. The ESPR is the key instrument to develop a single market for sustainable products. Ecodesign requirements – i.e. harmonised performance and information rules – will be developed and adopted for the most impactful products on our market, to reduce their negative environmental impact and improve information. In addition, there will be measures to prevent destruction of unsold products and possible mandatory green public procurement (GPP) requirements, to boost demand for sustainable products and create lead markets.

The first ESPR working plan will identify priority products for the coming years (to be adopted by 19 April 2025). Products have been assessed on the basis of their potential contribution to EU environmental, climate and energy efficiency policies, and other criteria set in the ESPR. The draft ESPR working plan[196] presented to the Ecodesign Forum on 18 February 2025 includes a number of energy-related products such as displays, smartphones and tablets, and horizontal measures on repairability, recyclability and recycled content. Those are likely to include consumer electronics in their respective scopes.

All in all, the ESPR will help to ensure that the materials, resources and value of products are maintained in the economy for as long as possible and to accelerate progress towards a single market for sustainable products, reinforcing the EU's overall resilience and competitiveness.

Measures under the ESPR will build on the Ecodesign Directive's and the Energy Labelling Regulation's successful examples, such as those of smartphones and tablets. As of 20 June 2025 those products, when put on the EU market, will have to display an energy label containing information on their energy efficiency, battery longevity, protection from dust and water, and resistance to accidental drops. This is also the first time that a product placed on the EU market will be required to display a reparability score (also present on the energy label). This will help EU consumers make more informed and sustainable purchasing choices and encourage sustainable consumption.

---

[194] UNCTAD, '2024 Digital economy report', 2024.
[195] UNITAR, 'The global e-waste monitor', 2024.
[196] European Commission, Group of experts on eco-design for sustainable products and energy labelling, 2025.

Green AI initiatives

The AI Office is managing a study called 'Development of a study to measure and foster energy efficient and low emission artificial intelligence in the EU'[197]. The final results will be obtained by summer 2026 and will focus on four main objectives. First, a literature review must be carried out to explore the carbon footprint of AI, covering all life-cycle stages, including the production of hardware. The carbon footprint should be estimated in accordance with Recommendation (EU) 2021/2279. Second, a measurement framework for the energy consumption of AI must be developed to identify common ground to make the energy consumption of different AI applications comparable, in both the development and application stages. Third, an enforcement concept must be developed to ensure compliance and conformity. To leverage synergies and foster coherence, the governance framework should align with existing or forthcoming legally binding procedures and requirements and the governance put in place for them. It will be necessary to analyse different governance settings, along with the functions of the bodies and detailed cost and time estimates for each scenario. A comprehensive implementation framework must be designed to guide the assessment process for entities that would fall under the provisions of the AI Act or the AI energy and emission label. This implementation framework should encompass various aspects (i.e. measurement methodology, definition of test standards and procedures for testing AI systems, ensuring consistency, accuracy, representativity and reproducibility of measurements). Fourth, support must also be provided for the design of a repository showcasing the energy-efficient design of AI systems. The repository will highlight the development of best practice and operation solutions for energy-efficient AI, including computing hardware. It will further enable coders to download or copy code content (e.g. Github, HuggingFace), fostering the practical implementation of energy-efficient AI practices.

3.2.2 Connectivity

Connectivity is a central pillar of the twin transitions. Telecommunications contributes to sustainability challenges through its life cycle impacts on climate, energy consumption, and the environment, primarily due to rising traffic demand and the energy required for data transmission and computing. Additionally, the complexity and scale of telecommunications infrastructure create significant issues related to greenhouse gas emissions, e-waste, and circular economy practices. While the energy consumption of communications networks looks set to keep increasing in the next few years, the carbon footprint is expected to increase only modestly[198] or to stabilise, depending also on the overall transition to renewables in the EU in the coming years and on the effectiveness of the circularity measures applied to the ICT sector.

In 6G research, energy efficiency will be an important design criterion ('efficiency by design'). In the longer term, new transmission technology and low-power cells are promising to ensure that, even with the massive growth in data expected, energy consumption levels of future networks will not be significantly higher than those of today's networks. However, in the value chain of communication services and devices, home devices continue to present the biggest sustainability challenge. About

[197] European Commission, 'Artificial Intelligence Act: Call for tenders to measure and foster energy efficient and low emission artificial intelligence in the EU', 2024.
[198] International Energy Agency 2022.

85% of the carbon footprint of smartphones over their lifespan is expected to result from their production and distribution and only 15% from their usage[199].

Under the 2022 Digitalising the Energy System Action Plan[200], the Commission is to explore the possibility of developing common indicators to enable the monitoring and benchmarking of the energy consumption and environmental footprint of communications networks. In March 2024, the Commission delivered on this task in an in-depth technical report[201], which recommended eight out of the 19 sustainability indicators analysed. Building on this, the Action Plan further calls on the Commission to establish an **EU Code of Conduct for the sustainability of telecommunications networks**. The Commission has been closely involving stakeholders with relevant expertise, in particular through a workshop on 6 May 2025. The Commission also involved standardisation experts via the StandICT project, which is funded by Horizon Europe. At Member State level, this work is supported, in particular, by a study carried out by the German National Regulatory Authority (BNetzA) on the comparability of sustainability standards of telecommunications infrastructure. The Commission plans to publish the EU Code of Conduct by the end of 2025, as forecast in the Digitalising the Energy System Action Plan. In its December Conclusions on the 2024 White Paper 'How to master Europe's digital infrastructure needs'[202], the Council called upon the Commission 'to consider proposing a target on green digitalisation in the context of the review of the Digital Decade Policy Programme, based on an agreed monitoring methodology'. It is recommended that Member States closely align any national initiatives with the work on the upcoming EU Code of Conduct.

3.2.3 Semiconductors

Semiconductors are the key enablers of the dual digital and green transitions and are essential for achieving sustainability goals by enabling energy-efficient technologies in renewable energy, smart grids, and electric vehicles (EVs). They reduce energy consumption through low-power technologies and environmental sensing, while advanced materials enhance efficiency in power electronics. These innovations support the EU Green Deal and global efforts to cut carbon emissions. On the other hand, semiconductor manufacturing faces significant sustainability challenges, primarily due to its high energy consumption, extensive water usage, and reliance on hazardous chemicals. Fabrication plants consume vast amounts of electricity, leading to substantial greenhouse gas emissions. Additionally, the industry depends on perfluoroalkyl and polyfluoroalkyl substances (PFAS), known as 'forever chemicals,' which pose environmental and health risks due to their persistence and toxicity. Addressing these challenges requires a comprehensive approach, including transitioning to renewable energy sources, developing alternative materials, and enhancing resource efficiency throughout the manufacturing process.

The **Industrial Alliance on Processors and Semiconductor Technologies**[203] is a collaborative European initiative aimed at strengthening the semiconductor industry's competitiveness and sustainability. It was launched in July 2024. Within the alliance, a dedicated Working Group on Sustainability and PFAS has been created with the objective of promoting strategies to mitigate PFAS-related environmental and health impacts, fostering research and development of suitable

[199] JRC, 2020; European Environmental Bureau, 2019; Journal of Cleaner Production, Volume 177, 2018.
[200] Digitalising the energy system - EU action plan, COM(2022) 552 final, 2022.
[201] Joint Research Centre European Commission, 'Green and sustainable telecom networks', 2024.
[202] European Council, 'Digital infrastructure: Council approves conclusions on the Commission's White Paper', 2024.
[203] European Commission, 'Industrial Alliance on Processors and Semiconductor Technologies', 2025.

alternatives, and advising the European Commission on policy actions to ensure compliance with environmental regulations while considering industry constraints.

The **European Chips Act**[204], which entered into force in September 2023, aims to strengthen Europe's semiconductor supply chain security and resilience while driving sustainable innovation. Under Pillar 2, it facilitates investments in first-of-a-kind semiconductor manufacturing facilities in Europe. To qualify, these facilities must introduce new and advanced manufacturing processes or products, which include measurable reduction in the consumption of energy, water, and chemicals and improvements in recyclability. In general, the European Commission supports dedicated research initiatives focused on sustainable manufacturing practices, aiming to improve resource efficiency in semiconductor production and find alternatives to environmentally harmful substances.

The **Chips Joint Undertaking** (Chips JU)[205], which was launched on 30 November 2023, is the key implementation vehicle of Pillar 1 of the Chips Act, driving R&D, innovation, and capacity building to strengthen Europe's semiconductor ecosystem. The Strategic Research and Innovation Agenda for the Electronic Components and Systems industry (ECS-SRIA) provides the strategic roadmap for the Chips JU, aligning research with Europe's technological and sustainability goals. The SRIA emphasises sustainability as a core objective, focusing on enhancing energy performance and minimising the environmental footprint of the industry, aligning with broader environmental and climate goals. Specific strategies include the adoption of advanced engineering tools to improve resource efficiency and minimise waste, as well as eco-design and circular economy principles, such as the 9R framework, to reduce environmental impact. The Chips JU and its predecessors, the Electronics Components and Systems for European Leadership Joint Undertaking (ECSEL JU) and Key Digital Technologies Joint Undertaking (KDT JU), have actively promoted sustainability in semiconductor manufacturing through dedicated R&D focus areas and projects supported with Horizon Europe funding. In its 2024 Work Programme, the Chips JU included a call entitled 'Sustainable and Greener Manufacturing'[206], allocating EUR 15 million to support a collaborative project aimed at reducing the environmental footprint of semiconductor manufacturing. The selected project, called Genesis, has recently started; it is led by the French Alternative Energies and Atomic Energy Commission (CEA) and involves 60 partners from 12 Member States. Genesis aims to enhance the sustainability of ICT manufacturing by improving process efficiency, recyclability, and resource management. It focuses on reducing the use of critical raw materials (CRMs) and eliminating toxic compounds like PFAS, while developing innovative material recovery solutions. By integrating eco-friendly processes and circular economy principles, the project seeks to minimise waste, lower environmental impact, and promote a greener semiconductor industry. Other relevant projects (like Sustronics, and EECONE) focus on circular economy principles, bio-based materials, and reducing electronic waste. These initiatives promote energy-efficient, repairable, and recyclable electronics, in alignment with the EU's sustainability goals.

Furthermore, Horizon Europe and the EIC also support sustainable semiconductors and electronics through targeted calls, such as the Pathfinder Challenge on Responsible Electronics of the EIC 2024

---

[204] Regulation (EU) 2023/1781 of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act).
[205] Chips Joint Undertaking, Empowering Europe's Semiconductor Industry, 2023.
[206] Chips Joint Undertaking, 'Sustainable and Greener Manufacturing', 2024.

Work Programme, which funds research on eco-friendly components and systems and supports semiconductor start-ups with sustainable and energy-saving innovations.

3.3 Development of concrete digital policies and tools for the green transition

Emerging evidence shows that digital technologies are delivering tangible efficiency gains for sustainability across Europe. The European Commission's Joint Research Centre estimates that today's digital tools could, if optimally deployed, cut 15-20% of total greenhouse gas emissions[207]. According to Eurostat (2025)[208], renewable energy sources accounted in 2023 for 45.3% of the EU's gross electricity consumption – the highest share on record – aided by smart grids and AI-driven management that help integrate wind and solar energy[209].

Artificial intelligence is increasingly being deployed across Europe to optimise resource use at scale, and also to support people in making more climate-conscious choices. For example, AI-powered systems for smart home energy management, food waste reduction, and sustainable mobility planning are demonstrating measurable environmental benefits. In relation to greenhouse gas emissions, AI is estimated to mitigate global emissions by 5-10%[210]. AI-powered consumer tools – such as eco-friendly routing – are enabling significant emissions reductions by optimising everyday decisions. These systems can suggest driving routes that maintain smoother speeds, avoid congestion, and minimise elevation changes, while preserving comparable arrival times. When applied in logistics, these systems can reduce emissions by up to 25%[211]. These tools contribute not only to individual behavioural shifts but also to systemic decarbonisation across transport, energy, and consumption patterns – all essential pillars of the EU Green Deal and the Digital Decade objectives.

In 2024, the European Union made tangible progress in implementing policies that align the digital transformation with its climate and sustainability goals. Moving beyond vision statements, the focus shifted to the concrete implementation of regulatory frameworks, data ecosystems, digital infrastructures, and intelligent tools designed to support emissions reduction, circularity, and resilience.

3.3.1 Laying the foundations: Regulation and standards for twinning the green and digital transitions

A strong regulatory foundation is key to ensuring that digitalisation promotes sustainability by design. In 2024, the EU strengthened this foundation through key legislation and standard-setting initiatives.

The Energy Efficiency Directive (EED) now requires large data centres (with capacity of more than 500 kW) to report on key performance indicators (KPIs) related to energy use, water consumption, cooling efficiency, and renewable energy uptake. A Delegated Act adopted in spring 2024 introduced a formal reporting scheme, standardising metrics such as Power Usage Effectiveness (PUE), Water

[207] Joint Research Centre, European Commission, '5 digital solutions for a greener Europe', 2023.
[208] Eurostat, '2023: record-breaking increase in renewable electricity', 2025.
[209] European Parliament, 'Increasing Flexibility in the EU Energy System', 2025.
[210] Boston Consulting Group, 'Reduce Carbon and Costs with the Power of AI', 2021.
[211] Mandal J. & Asim Mohammed, I., Implementation, International Journal of Supply Chain Management, 2024.

Usage Effectiveness (WUE), and Renewable Usage Effectiveness (RUE). A second Delegated Act is under preparation to introduce a labelling system for data centre energy performance, with recommendations expected in Q3 2025.

At the same time, the Ecodesign for Sustainable Products Regulation (ESPR), adopted in June 2024, introduced the Digital Product Passport (DPP) to enhance product transparency and sustainability. The CIRPASS project concluded in March, paving the way for CIRPASS-2, launched in May 2024. This follow-up initiative will demonstrate the functioning of DPPs in 13 pilot settings and provide evidence for future standardisation.

Meanwhile, the AI Act entered into force in August 2024. While focused on safety and fundamental rights, it also includes provisions for resource efficiency, requiring providers of general-purpose AI models to report energy and computational resource consumption. The Commission is empowered to adopt Delegated Acts to harmonise methodologies for calculating energy use, enabling comparability and accountability.

A key milestone was the publication in April 2024, by the European Green Digital Coalition (EGDC), of a science-based method to estimate the net environmental impact of digital solutions in major sectors of the economy such as energy, transport, construction, agriculture, smart cities, and manufacturing. This work was done by the EGDC Pilot Project in the framework of the European Action plan on Digitalising the EU energy system, which supported relevant organisations and experts to work with the EGDC members to develop the Net Carbon Impact Assessment Methodology for ICT Solutions. For the first time there is a detailed and agreed methodology to calculate both the negative and positive carbon impact of digital solutions such as those used in the context of smart cities. If the net impact is positive, that provides the necessary evidence to policymakers and financial actors to support the scale-up of such solutions. In March 2025 the new EGDC Pilot 2 started, which will calculate 50 case studies from different sectors including smart cities settings and bring financial institutions to develop eligibility criteria for climate (green) financing of the deployment of proven green digital (including AI-based) solutions.

Together, these legislative and standardisation efforts define the boundaries and expectations for climate-aligned digitalisation. To support them, the EU is also investing in infrastructure and data ecosystems that make such compliance feasible and scalable.

3.3.2 Building the Infrastructure: Data spaces and digital backbones

To translate policy into practice, the EU has supported the development of shared data infrastructures and enabling platforms to support sustainability-driven innovation.

In the energy sector, six ongoing projects funded by Horizon Europe are preparing the ground for the deployment of the energy data space. Five of them develop detailed use cases, identify building blocks and define interoperability requirements. A coordination and support action will seek to establish an interoperability framework and an open, cross-domain community of stakeholders to work on developing, testing and deploying interoperable energy services. The Smart Energy Expert Group was launched in October 2024 to support the establishment and governance of the energy data space, through its 'Data for Energy' subgroup. A new project that started in April 2025, funded by the Digital Europe programme, will work on the deployment of the energy data space.

The EU also invested EUR 56 million in flagship projects including TwinEU (a digital twin of the EU's electricity system), ODEON, and HEDGE-IoT, all of which leverage AI and IoT to increase system efficiency and resilience. Complementing these efforts, the ECLIPSE project integrates real-time

smart meter data into customised applications that help users monitor and reduce consumption, improving both household energy efficiency and grid stability. A catalogue of smart grid indicators is also being developed to measure the performances of smart grids both at distribution and transmission level.

Beyond energy, data spaces have expanded in mobility and agriculture. The Common European mobility data space (EMDS) entered its deployment phase, with the deployEMDS action implementing 16 use cases across nine cities and regions. These include optimising public transport, planning zero-emission zones, and enabling multimodal travel solutions.

In agriculture, the Common European Agricultural Data Space (CEADS) advanced significantly. The AgriDataSpace preparatory action concluded in Q2 2024, and the deployment phase will begin in Q2 2025. The CEADS will enable AI-based innovations to improve resource efficiency, reduce inputs such as water and fertiliser, and support sustainable farming practices.

These infrastructures provide the connective tissue for data-driven innovation. Once in place, they enable the development of targeted digital tools that serve the public, ecosystems, and climate goals in tangible ways.

3.3.3 Digital tools for climate monitoring, urban planning, and resilience

Building on these digital foundations, 2024 saw the roll-out of powerful tools and applications supporting climate adaptation and sectoral decarbonisation.

Destination Earth (DestinE) and the EU Digital Twin Ocean completed their first implementation phase in June 2024, releasing a pre-operational version of their digital twin platform. It offers high-resolution simulations, tailored climate impact data, and on-demand 'what-if' scenario analysis to support evidence-based adaptation policies, long-term resilience planning and scenarios for sustainable economic activities.

The Horizon Europe-funded WATERVERSE project is developing a European water data management ecosystem. The project focuses on real-world case studies in six countries, including predicting water quality (NL), digital village twin for flood protection (DE), smart water tools and risk management (FI), water digital twin and water analytics tools (CY), management of the water cycle and open innovation (ES) and combined sewer overflow performance (UK).

Horizon Europe funded project's clusters (19 currently active from WP2021) develop improved uptake and applications on key environmental and climate issues (freshwater ecosystems, fires, climate intelligence), making use of combined AI and satellite / in-situ observations with further developments planned in upcoming WPs.

Meanwhile, the Green Deal Data Space (GDDS), supported through the Digital Europe Programme, is integrating over 500 datasets across climate, biodiversity, pollution, and circular economy areas, helping stakeholders monitor progress against Green Deal targets.

In urban sustainability, the new LDT-CitiVERSE-EDIC will receive within the EU LDT toolbox a complete set of digital services to be used together with the EU building dataset for AI-based impact assessment of New European Bauhaus strategies. The DEP project DigiNEB on the digital dimension of the NEB domain, completed in cooperation with the NEB Academy, will offer the LDT-CitiVERSE-EDIC practical opportunities for exploitation of its platform and services. The tools developed under the 2024 call on CitiVERSE projects will provide relevant input to further develop the EU Virtual

Worlds ecosystem. This input will be promoted with the support of the LDT-CitiVERSE-EDIC for reuse and quick uptake in this key area.

These applied tools show the practical value of high-quality data and computing infrastructure, turning EU investments into visible and impactful change on the ground.

3.3.4 Sustainably shaping AI, emerging tech and circular innovation

Alongside deployment, the EU is embedding sustainability in the design of future digital technologies.

The Apply AI Strategy, which was being developed in 2024, will promote the use of AI in industrial and environmental domains, including traffic optimisation, precision agriculture, and renewable integration. Support is being mobilised through AI Factories, common data spaces, and computing infrastructure.

The next phase of DestinE will add machine-learning demonstrators for climate prediction and launch user-facing tools like 'forecast in a box' and a climate chatbot. These tools will enhance public engagement and decision-making in climate policy.

Efforts in circularity are also intensifying. The CIRPASS-2 project will deliver recommendations for standardising DPP implementation, while upcoming regulations under the Ecodesign Directive for Digital Devices will introduce requirements for repairability and recyclability. Extended Producer Responsibility (EPR) schemes are under consideration to strengthen the end-of-life management of electronic products.

As the EU continues to invest in frontier digital technologies, the integration of sustainability principles at design phase is becoming the norm – ensuring long-term environmental value alongside innovation.

3.4 Green/digital twin transition measures at Member State level

The year 2024 saw a wave of activity aimed at operationalising the green/digital twin transitions through national strategies, regulatory frameworks, and sector-specific deployments. This shift is no longer limited to high-level ambitions or isolated pilot projects. Instead, national strategies, regulatory frameworks, and sector-specific deployments are increasingly reflecting a dual focus: enabling digital transformation while simultaneously advancing environmental objectives. The resulting activity signals the beginning of a more mature and systemic phase of policy implementation in the context of the Digital Decade.

3.4.1 Digital and green transitions in the national roadmaps

In their national Digital Decade roadmaps, 19 Member States included 67 measures contributing to the green transition. These measures focus on greening the digital transition by making digital technologies and infrastructure more energy-efficient and on using digital technologies and infrastructure to leverage the green transition. Among those measures, more than 30 are specifically designed for the objectives of the green transition.

In total, 17 measures from the repository are scheduled to begin in 2024 or 2025, reflecting the fact that Member States are no longer preparing for the green/digital transition – they are acting on it.

Among the most tangible of these actions are national efforts to reduce the environmental footprint of digital infrastructure. Ireland's *Shared Government Data Centre*[212], which will continue to be developed through 2025, aims to consolidate disparate public IT systems into a centralised, cloud-based infrastructure that significantly reduces energy consumption. Luxembourg has likewise pushed forward the green-digital transition by developing a National Energy Data Platform. Required by law and implemented by the Transmission System Operator CREOS, the platform serves as a central hub for exchanging energy market data across electricity and gas sectors. It aims to increase data accessibility for customers and market actors, improve the efficiency of market processes, and support better regulatory reporting. By enabling secure, standardised, and transparent data flows, the platform lays the digital foundation for a more sustainable and competitive energy system. This type of investment reflects a broader shift across Member States – from siloed, voluntary greening initiatives to principles of energy efficiency and sustainability embedded in core digital governance structures. Rather than treating environmental considerations as secondary or external, public authorities are beginning to treat sustainability as foundational to digital infrastructure design.

Beyond infrastructure, several Member States are increasingly adopting strategic frameworks that embody an emerging consensus that digitalisation must be mobilised to enhance environmental monitoring, reduce ecological footprints, and foster circular economic models. In this regard, France has made notable advances. Its *2030 Acceleration Strategy for Eco-responsible, Competitive and Sovereign Digital Technology* sets out a long-term national vision to anchor ecological transition and technological sovereignty at the heart of digital policy. Under this strategic umbrella, France has reinforced its leadership on green ICT through a series of targeted measures included in its adjusted Digital Decade roadmap. These include the first national reference framework on the environmental impact of AI, which has led to the creation of a frugal AI standard for measuring and reducing energy and material use, and the introduction of a EUR 20 repairability bonus for highly repairable digital devices. Together, these initiatives represent a coordinated effort to integrate environmental responsibility into digital innovation, product design, and market incentives.

European Lighthouse of AI for Sustainability

ELIAS[213]**,** funded by the European Union, aims to establish Europe as a leader in AI research that drives sustainable innovation and economic development. For this purpose, it has created a Network of Excellence of 34 partners in 17 countries that is connecting researchers in academia with practitioners in the industry. Use cases include, e.g.: i) AI for building optimisation: cost reduction by reducing energy consumption through smart control systems, which requires both control algorithms and prediction of actual consumption on the basis of historical patterns and metadata, such as meteorological information; ii) AI for forecasting the state of vegetation: studying AI-based predictions of the effects of climate extremes on ecosystems, which can then be translated into crop harvest, forest health and water balance forecasts. The project will run for four years.

In 2024, Member States began operationalising the green-digital nexus not only through strategic frameworks but also through concrete reforms that reflect systemic integration. Italy's '*Transition 5.0*' Plan stands out as a flagship measure, linking digitalisation and sustainability through a

[212] European Commission, 'Development of a Shared Government Data Centre', 2025.
[213] ELIAS – Lighthouse of AI for Sustainability.

EUR 12.7 billion programme running over 2024-2025. The plan introduces a performance-based tax credit for investments in production structures, conditional on achieving measurable reductions in energy consumption. Building on the earlier Transition 4.0 Plan, it supports the adoption of energy-efficient technologies, digital systems for monitoring consumption, and renewable energy solutions, while also funding workforce training specifically in skills that support the sustainable transformation of production processes. Together, such frameworks illustrate how Member States are institutionalising the green-digital agenda at both strategic and operational levels, embedding environmental goals in the core of national digitalisation policies. In Slovenia, reforms have focused on regulation: the country's Green Public Procurement Regulation has been modernised to incorporate digital tracking systems that ensure compliance with environmental criteria, making public procurement an engine of green-digital alignment.

A number of measures starting in 2024 demonstrate how Member States are deploying digital technologies directly to achieve climate and environmental goals. For example, Denmark launched three distinct but complementary measures under this objective. The *'Establishment and Operation of a Supply Digitalisation Programme'* aims to create frameworks and regulations for how data is collected, structured and made accessible in the utilities sector, starting with data from the electricity, heating and water sectors. Simultaneously, the measure *'Monitoring Groundwater and Ensuring Clean Drinking Water'* leverages data analytics to enhance knowledge about drinking water supply, and *'Improved Transition to Electric Vehicles and Alternative Fuels Through Open and Standardised Data'* will establish an IT solution to display and distribute standardised data from publicly accessible charging points and fuelling stations in Denmark. Thus, it appears that some MS have adopted the use of digital technology to monitor the ecological transition in their territory by capturing and sharing data of environmental interest.

These initiatives are a decisive move toward sector-specific deployment of digital tools – not as pilots, but as embedded components of environmental policy. They signal a phase of operational maturity where digital technology is not only enabling the green transition but actively shaping its implementation.

Funding and MCPs to twin the green and digital transitions

A wide range of EU funding instruments and Multi-Country Projects (MCPs) have been mobilised to accelerate the deployment of digital technologies for sustainability and climate action. These initiatives focus on building interoperable infrastructures, platforms, and datasets to support sectors such as energy, mobility, construction, and manufacturing in achieving the objectives of the Green Deal and the Digital Decade.

Among the key instruments, the establishment of European Digital Infrastructure Consortia (EDICs) represents a strategic approach to scaling up common digital assets across Member States. In this context, the LDT-CitiVERSE-EDIC, set up in February 2024 and launched in Valencia in December 2024, exemplifies how EDICs can provide operational platforms for reusing EU-funded services, tools, and data infrastructures. While initiated in the urban context, the EDIC's architecture – built on the first SIMPL-based EU Data Space – is designed for broader reuse, including in sectors such as energy efficiency, or sustainable construction.

The Digital Europe Programme (DEP) continues to serve as a major funding source for digital sustainability tools, including projects like DigiNEB, which developed the digital dimension of the

New European Bauhaus (NEB) and created synergies with the NEB Academy to ensure training and practical uptake. Outputs from DigiNEB and the 2024 CitiVERSE call will feed into the development of the EU Virtual Worlds ecosystem, providing immersive environments for scenario testing, digital twins, and AI-supported impact assessment across domains.

3.4.2 Sharing of best practices within the Digital Decade Policy Programme

The Green IT cluster of the Digital Decade Best Practice Accelerator has been led by France since it was launched during the first workshop in July 2024. Since then, two more workshops have taken place at which several Member States presented their best practices to address the environmental impact of data centres, to measure the impact of ICT, and to contribute to the circular economy and the collection of electronic waste.

France has three best practices on the twin transition field: i) the **General Policy Framework for the Eco-design of Digital Services**[214], which targets ICT professionals and sets out 78 criteria and best practices to apply eco-design principles in the development of a service and to draft an Eco-design declaration; ii) the development and availability of **Product Category Rules** (PCRs)[215] for environmental evaluation and labelling, aiming to ensure the comparability and robustness of environmental information provided to consumers, covering the entire product life cycle; and iii) the **Alt IMPACT Communication Campaign**[216] to raise public awareness about the environmental impact of digital technologies, which is part of the measures taken by the French government to promote digital sobriety (such as the 'Digital and Environment' roadmap and the 2021 REEN law aimed at reducing the environmental footprint of digital technology).

The Netherlands presented its **Sustainable Digitalisation Action Plan**[217] published in July 2024. It outlines 44 specific actions along three main action lines that seek to make the digital sector more sustainable, while simultaneously leveraging digitalisation for sustainability by improving the efficiency of production processes, optimising the use of existing resources and enabling circular use of raw materials and resources. These actions unify efforts from both the government and the private sector, building on existing policies without requiring additional resources or capacity.

Finland presented its **measures to increase the knowledge base on the environmental handprint and footprint effect of the ICT Sector**[218]. This best practice was put forward in response to the lack of reliable and comparable data that Finland identified as one of the challenges when drawing up its national climate and environmental strategy for the ICT sector (published in 2021).

Luxembourg presented its **Product Circularity Data Sheet (PCDS),** a tool designed to provide detailed information about the circular characteristics of products, such as their recyclability and durability, and the use of recycled materials, which is aligned with the horizontal requirements of the ESPR.

---

[214] ARCEP & ARCOM, 'General policy framework for the ecodesign of digital services', 2024.
[215] ADEME, 'Ecolabelling', 2025.
[216] ADEME, 'Towards real Green IT', 2022.
[217] Netherland Central Government, 'Sustainable Digitalisation Action Plan', 2024.
[218] TIEKE Finnish Information Society Development Centre, 'Green Metrics for Public Digitalization Acquisitions – MitViDi', 2023.

3.4.3 Conclusion and way forward

During the 2024 Digital Decade year, the EU established a solid foundation of legislation, strategic direction, and funding to accelerate the green and digital transitions. That foundation has been translated into the deployment of specific instruments – such as the **Ecodesign for Sustainable Products Regulation**, the **Digital Product Passport**, and the **Cloud and AI Development Act** – that directly support climate goals through digitalisation. The EU has also provided interoperable infrastructures and data ecosystems, such as **TwinEU** and the **GDDS**, and emerging common data spaces for energy, mobility, and agriculture, enabling a new generation of AI-powered tools that contribute to circularity, emissions reductions, and environmental resilience. These EU-level efforts have shifted the focus from potential to delivery, and from isolated pilots to systemic implementation.

Digital technologies – when deployed under the right conditions – have provided measurable benefits: digital technology can help cut global emissions by 20%, outweighing the current 2% to 4% of global emissions caused by the sector. Other benefits include emissions reductions of up to 25% in logistics through AI-driven routing, 30% water savings via smart irrigation systems, and enhanced energy efficiency through virtualisation and smart grids. These benefits come not at the expense of social outcomes, but often in synergy with them – improving access, affordability, and transparency. Crucially, methods to assess their net climate impact are now available and maturing. The **Net Carbon Impact Assessment Methodology**, developed by the **European Green Digital Coalition (EGDC)**, and the forthcoming AI energy/emissions label, along with Member State initiatives like the ADEME (France) lifecycle-based tools, provide a common ground on which to evaluate the real contribution of digital solutions to environmental goals.

At national level, Member States have begun embedding these frameworks in tangible reforms. Measures such as **Italy's Transition 5.0 Plan**, **Luxembourg's National Energy Data Platform**, and **France's Frugal AI standard** illustrate how EU support has been translated into localised, impactful action. In total there are now more than 30 measures specifically designed for the objectives of the green transition. These initiatives reflect an increasing alignment between national strategies and EU ambitions and show how Member States have provided not just implementation capacity, but also innovation leadership and best practices, in particular through the Digital Decade Best Practice Accelerator.

Looking ahead, the way forward lies in scaling up these successes, anchoring them in enforceable standards, and ensuring that digitalisation contributes net-positive value for the climate. While the EU has provided the architecture, full alignment across levels of governance and a persistent focus on measurable impact, responsible innovation, and sustainability by design are still needed.

4 Coherence and synergy: aligning digital policies and funding at different levels

The Digital Decade includes a joint commitment to ensure that digital policies, measures and programmes which are relevant to the EU's digital transformation are considered in **a coordinated and coherent way** in order to fully contribute to the Digital Decade objectives, while **avoiding overlaps and minimising administrative burdens.**

This chapter offers an overview of the EU's progress towards achieving the above-mentioned objectives, structured across four key dimensions. First, it examines the development of better and lighter digital legislation, encompassing efforts to eliminate overlaps and unnecessary burdens, simplify existing rules (including through digital solutions), and improve governance. Second, the chapter analyses the effectiveness of digitalisation funding, identifying potential improvements and synergies between relevant programmes and instruments. Third, it reviews the implementation and dissemination of digital policy across governance levels, emphasising enhanced collaboration between the Commission, regions, and cities. Finally, it outlines the EU's international digital strategy, detailing how the EU promotes its vision, interests, and values globally while fostering cooperation to strengthen its international standing in the digital arena.

4.1 Better and lighter digital legislation

4.1.1 Overlaps and unnecessary burdens

The European Commission's President, Ursula von der Leyen, has outlined in the '*Political Guidelines for the next European Commission 2024-2029*' **a comprehensive plan to ensure prosperity and competitiveness in Europe**, with a focus on making business easier and deepening the Single Market.

One of the key barriers to competitiveness is the administrative burden, which can hinder the growth of small and medium-sized enterprises. The Commission recognised that SMEs face too many complexities and bureaucratic hurdles, which can limit their ability to scale up and compete in the global market.

According to the European Investment Bank's Investment Report 2024-2025, **the cost of bureaucracy is a significant burden for EU firms, particularly for smaller enterprises**. In turn, simplification is one of the key drivers to consolidate Europe as a global leader in new technologies, alongside market integration and large-scale investment in innovation. The EIB Investment Survey (EIBIS), which provides detailed information from more than 12 000 European companies, specifies that about 86% of EU firms employ staff specifically to deal with regulatory compliance, at an average cost of 1.8% of turnover. The cost increases to 2.5% of turnover for SMEs. As a comparison, EU firms' spending on energy after the energy shock is equal to 4% of turnover.

To address this issue, **the Commission proposed to simplify legislation, reduce administrative burdens,** and introduce a new category of small mid-caps to support innovative companies. Moreover, the Commission's President appointed a Vice-President for Implementation, Simplification, and Interinstitutional Relations, whose task is to stress-test the entire EU *acquis* and eliminate any overlaps and contradictions, while instructing all Commissioners in their mission letters to ensure that existing rules are fit for purpose and focus on reducing administrative burdens and

simplifying legislation, with the goal of reducing reporting obligations by at least 25% – and for SMEs by at least 35%.

Executive Vice-President (EVP) Henna Virkkunen was specifically tasked in her letter with **deploying digital public infrastructure, notably by making the most of the EU wallet,** to ensure businesses can fully use the technology enabling them to speed up and simplify operations and reduce administrative costs. The EVP was also asked to present a European Data Union Strategy to ensure **a simplified, clear and coherent legal framework for businesses and administrations to share data seamlessly and at scale,** while respecting high privacy and security standards.

The Commission's 2025 Work Programme, adopted in February 2025, seeks to deliver on commitments outlined in the Political Guidelines and the mission letters. It was accompanied by the '*Communication on Implementation and Simplification*', in which the Commission outlined actions and tools to improve the implementation of EU rules. This initiative introduces the Omnibus Simplification Packages, whose aim is to streamline and modernise regulatory frameworks across the EU, reduce unnecessary complexities and foster a more innovation-friendly environment. There are three such packages in the Commission 2025 Work Programme: one on sustainability, another on investment simplification, and a third on small-caps.

Regarding actions focusing on digital policy, the Programme announced a simplification package that will have an impact on EU companies by streamlining cybersecurity reporting requirements and data-sharing obligations. It will include a review of the Cybersecurity Act to simplify cybersecurity legislation, facilitating multipurpose reporting and avoiding duplications. In addition, the package will address existing data rules for the purposes of ensuring a coherent legal framework for data sharing, while respecting security and privacy standards.

The Commission also proposed targeted changes to the General Data Protection Regulation (GDPR) as part of the **small midcaps package**. These changes aim to ease record-keeping obligations for SMEs and organisations with fewer than **750 employees**, while maintaining the core objectives of the GDPR. Further discussions with stakeholders are planned to explore potential additional simplification measures, but it is too early to anticipate whether further legislative proposals will follow later this year.

The 2025 Work Programme also included a **fitness check on the legislative *acquis* in the digital policy area** to be concluded in the last quarter of 2025. The fitness check will determine if the expanded legal framework for the digital environment meets the needs of businesses, particularly small and medium-sized enterprises (SMEs) and small mid-caps.

As part of its 2025 Work Programme, the Commission published a list of 51 initiatives for this year and details of 37 pending files it plans to withdraw, including the **AI Liability Directive.** The fitness check on the legislative *acquis* in the digital policy area is expected to conclude in the last quarter of 2025.

4.1.2 Digital solutions for burden reduction and simplification

The potential of digital solutions for reducing administrative burdens is recognised in two key reports on EU competitiveness and the Single Market, published last year. The '*Much more than a market*' report (also known as the 'Letta report'), published in April 2024, advocates accelerated digitalisation in authorisation and reporting procedures, because it will significantly reduce the administrative burden for businesses and workers engaging in cross-border activities. It will also reduce the amount of paperwork and the space and energy required to store and move it. The '*Future of European*

competitiveness' report (also known as the 'Draghi report'), published in September 2024, concurs by proposing the introduction of digital solutions for monitoring, reporting and verification processes in the case of importers and third-country producers and by linking them to existing supply chain and enterprise management systems.

A key part of the Commission's efforts to meet these expectations is the development of European Business Wallets as a cornerstone of doing business simply and digitally in the EU, providing a seamless environment for economic operators to interact with all public administrations, as stated in the Competitiveness Compass. The use of digital tools and AI to power simplification efforts at government level must be facilitated, with full cross-border interoperability among public-sector bodies' solutions. Wherever possible, reporting must move to digital formats based on standardised data.

Building on the EU Digital Identity Framework, the **European Business Wallet will be a horizontal enabler of Europe's competitiveness**. Conceptually, the Business Wallet will emulate and complement the key benefits of the European Digital Identity Wallet for natural persons. The initiative addresses key problem drivers – fragmentation of national portals, inefficient administrative processes, and cumbersome compliance obligations – by providing a single, secure, interoperable, cloud-based identity solution. It does so by enabling economic operators to identify and authenticate themselves, share credentials, and receive official notifications across the EU using a harmonised, legally recognised identity infrastructure. This will ensure efficient reporting, accelerate transactions, and enhance trust in EU-wide digital operations that ultimately will support the effective functioning of the Single Market and increase European competitiveness.

Another key initiative of the Commission is the implementation of the Single Digital Gateway (SDG). The Your Europe portal – its interface and brand name – offers access to information about rights, rules and e-Government services for Europeans to navigate and simplify their cross-border activities in the EU single market. This includes activities such as studying, living, working or doing business. The 'Only-Once Technical System' (OOTS) will, on top of this, reduce the time and costs involved in dealing with cross-border paperwork by automatically mapping the (structured or unstructured) documents or data needed for online procedures and by transferring them directly and securely from one authority to another across borders upon request. A 2024 study shows that using the OOTS will cut SMEs' cross-border administrative costs and time by more than half[219].

The forthcoming European Business Wallet, Single Digital Gateway, the OOTS and the EU Digital Identity Wallet will create a cohesive ecosystem of digital solutions that simplify various aspects of life for Europeans.

Another important initiative relying on digital solutions to reduce friction and cost related to daily operation, while improving security and enhancing EU sovereignty, is the Digital Euro. The proposed legislation will allow users to use their European Digital Identity Wallets to verify their identity, confirm their payments, and grant permissions with ease, enabling seamless digital euro transactions and opening accounts. Moreover, the integration of the digital euro with these wallets will provide users with a secure and private gateway to access a range of digital services, both public and private, while also reducing operational costs for businesses.

---

[219] OOTS,' EU SMEs and self-employed workers could save time and money when expanding abroad thanks to the Once-Only Technical System '. 2024.

The Single Market is progressively evolving into a space for paperless and document-free interactions between citizens and public authorities, facilitated by the harmonisation of data formats across the EU. This digital transformation significantly impacts public procurement, where digital solutions simplify processes. The **Public Procurement Data Space** (PPDS), activated in September 2024, has become a crucial tool for understanding the Single Market and assists reporting and monitoring within the public procurement domain.

Finally, a **significant step towards simplifying and reducing administrative burdens**, particularly for SMEs, will be made with the implementation of the **VAT in the Digital Age** legislation, which was adopted on 11 March 2025. This legislation enables automated VAT reporting through e-invoicing, simplifying the extraction and processing of VAT-relevant data from electronic invoices. This streamlined approach not only applies to cross-border transactions but can also potentially be applied by Member States to domestic transactions. In addition, the European Commission is expanding the utility of e-invoicing to encompass sustainability reporting.

Following the sustainability reporting standards published by the European Financial Reporting Advisory Group (EFRAG) in December 2024, the Commission has initiated exploratory work on how e-invoicing can enhance the efficiency and accuracy of sustainability reporting, leveraging automatically extracted data from electronic invoices. This effort aligns with the Commission's policy on reusing existing data for compliance requirements, underscoring a broader move towards digital efficiency. The upcoming Business Wallet will also support the efforts to expand e-invoicing.

4.1.3 Simplification through improved governance

The Digital Decade Board (DDB) is the main forum for exchange of views and cooperation between the European Commission and the Member States regarding the Digital Decade. While its remit is even broader and covers all digital transformation issues and relevant legislation, policies, measures, actions and reports, the European Commission has also set up several other expert and special groups focusing on more specific aspects of the digital transformation.

There are 40 such bodies through which the European Commission works with and seeks assistance from the Member State authorities (almost 75% of cases), as well as individual experts and representatives of different organisations, including trade organisations and enterprises. They often play a role in implementing important legislation, such as the AI Act, the Digital Services Act, the Cyber Resilience Act, the Cyber Security Act, the eID Act, or the Chips Act, the European Media Freedom Act or connectivity and spectrum legislation. They act as coordination and governance bodies and provide an area for the exchange of views and cooperation to develop implementing measures. There are also groups that work on policy areas such as the digitalisation of health records, digitalisation of the energy system or safer internet for children.

Some Member States' representatives on the DDB raised concerns about the number and diversity of such groups, pointing to the potential overlaps and difficulty in ensuring proper follow-up of their activities given the limited resources of the national administrations. During the meeting of the Board on 6 March 2025, members of the DDB recognised its central role in fostering coordination, reducing fragmentation, and aligning measures with the capabilities of Member States, but some also highlighted the importance of collaboration between expert groups.

This matter will be explored further by the Commission and – as a first step – the Member States in the DDB will be informed about the various bodies established by the European Commission in the digital transformation to make sure that they have complete information and to help in internal

cooperation. In the future, this matter may be included in the scope of the review of the Digital Decade policy programme (DDPP), which should be completed by June 2026.

The DDPP provides a framework for the exchange of best practices between Member States, so they can learn from their experience and apply tried-and-tested solutions to common problems. There is no best practice cluster yet focusing on administrative burdens and simplification, but during the above-mentioned meeting of the Board several Member State representatives took the floor to share ideas on how the DDPP and the DDB can play a transformative role in simplifying processes for businesses and the public by addressing regulatory fragmentation, enhancing coherence, and reducing administrative burdens, particularly for SMEs.

Many emphasised the need for interoperable digital governance tools to simplify compliance and support small and medium-sized enterprises (SMEs). The Czech Republic (CZ) and Italy (IT) were among the advocates for this approach, proposing the development of a Single Digital Compliance Platform and a Single Digital Rulebook, respectively, to collate EU regulations and provide a user-friendly dashboard for businesses. Both countries also highlighted the importance of consolidating and codifying the EU's digital regulatory framework, with IT proposing a Pre-Legislative Consistency Check mechanism to prevent contradictions in new laws.

Other Member States, such as Belgium (BE) and Germany (DE), shared similar views on the need for digital transformation and regulatory simplification. BE proposed reusing existing digital infrastructure solutions across Member States to reduce costs, while DE emphasised the importance of reducing reporting burdens for businesses and aligning digital tools with the specific needs of Member States.

The Netherlands (NL) and Finland (FI) also contributed to the discussion, with NL underscoring the DDB's role in participating in the fitness check of the digital rulebook and FI highlighting the importance of fostering synergies between EU boards to streamline activities and reduce duplication. Many Member States also emphasised the need for improved coordination and support for SMEs, with IT proposing Digital Regulatory Sandboxes to enable SMEs to test solutions under regulatory supervision. BE and NL emphasised improving the visibility and accessibility of EU funding programmes for SMEs, with NL proposing EU-wide retail investment products and IT advocating fiscal incentives and private co-investment funds.

Hungary (HU) suggested leveraging stakeholder networks like Eurochambres and the Enterprise Europe Network to promote DDPP goals. Overall, there is a strong consensus among Member States on the importance of regulatory coherence, collaboration, and support for SMEs in achieving the goals of the DDPP. The Commission has acknowledged these suggestions and reaffirmed its commitment to exploring new procurement policies and ensuring a coherent application of State aid rules.

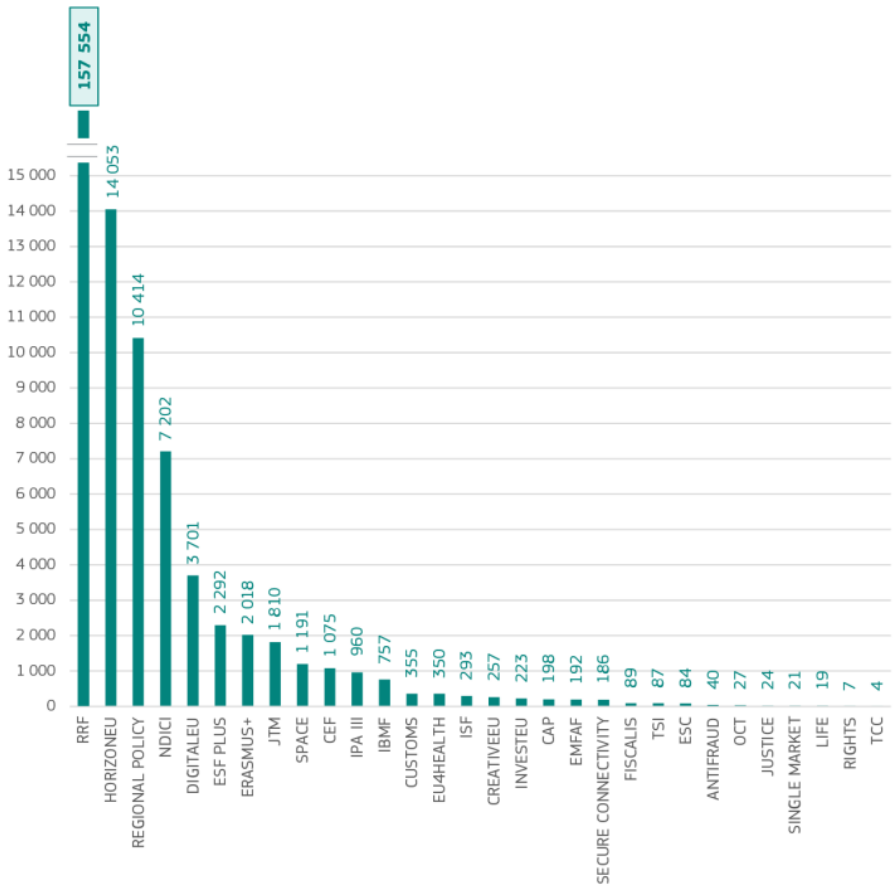
4.2 EU funding for the Digital Decade: state of play

4.2.1 Digital transition in the EU budget: update of the digital tracking

The digital transition is one of the top political priorities of the Commission, streamlined in the EU budget. An updated stocktaking exercise across all EU spending programmes for the 2021 to 2023 period highlights the substantial support the EU budget – including NextGenerationEU – is providing to all key aspects of the digital transition. The latest figures indicate that EUR 205.5 billion from the EU budget, representing nearly 17.5% of the total budget, was allocated to digital transition efforts

over that period. A major share of this investment came from the Recovery and Resilience Facility (RRF), which in the same period dedicated 24% of its total budget to digital-related investments and reforms.

Figure 35: Estimated contributions to the digital transition of the EU budget programmes, in 2021-2023 (cumulatively) (in EUR million)[220][221]



Source: Digital tracking – European Commission

The overall amount is likely to be greatly underestimated at this stage[222]. However, keeping this caveat in mind, the results show that almost all programmes that are part of the EU budget contribute to the digital transition.

---

[220] For readability purpose, the scale is broken: the RRF provides more than 10 times more support to the digital transition than the most contributing programme making the greatest contribution.

[221] The abbreviations used stand for: RRF – Recovery and resilience facility; HORIZONEU – Horizon Europe; NDICI – Neighbourhood, Development and International Cooperation Instrument – Global Europe; DIGITALEU – digital Europe programme; ESF PLUS – European Social Fund+; JTM – Just Transition Mechanism; SPACE – EU Space Programme; CEF – Connecting Europe Facility; IPA III – Instrument for Pre-accession Assistance III; IBMF – Integrated Border Management Fund; ISF – Internal Security Fund; CREATIVEEU – Creative Europe Programme; CAP – common agricultural policy; EMFAF – European Maritime, Fisheries and Aquaculture Fund; SECURE CONNECTIVITY – EU Secure Connectivity Programme; TSI – Technical Support Instrument; ESC – European Solidarity Corps; OCT – Decision on the Overseas Association, including Greenland; RIGHTS – Citizens, Equality, Rights and Values Programme; TCC – Turkish Cypriot community.

[222] Constraints on data availability allowed digital-relevant expenditure for the 2021-2023 period to be tracked for only 30 spending programmes (out of 48 with EU budget implemented in 2023).

In terms of thematic concentration, the EU budget is primarily supporting **government and public bodies in digitalising key sectors**, in particular health systems and transport. Significant efforts are also being made to support the **digitalisation of businesses**, to help the acquisition of (advanced and basic) **digital skills** and to support **research and innovation**, along with key **advanced digital infrastructure and technologies** (such as quantum computing, artificial intelligence and cloud/edge computing)[223].

4.2.2 The contribution to the Digital Decade targets: estimates 2025

The Joint Research Centre (JRC) examines the contribution of selected EU funding instruments to each of the Digital Decade targets[224]. This exercise considers the following programmes: the Recovery and Resilience Facility (RRF), Connecting Europe Facility (CEF Digital), Horizon Europe, the Digital Europe Programme (DEP) and Cohesion policy. As such, the analysis represents only a part of the broader EU budget and potential investments relevant to digital technology.

The estimates presented are indicative, but they offer valuable insights into the direction and scale of support provided to each Digital Decade target[225].

The results show that the mapped programmes play an important role in supporting the achievement of the Digital Decade targets. According to the mapping for 2021-2027, a total of **EUR 177.5 billion** from these five programmes is **directly aligned with the Digital Decade targets**. An **additional EUR 29.6 billion** support broader **digital objectives**, bringing the **total estimated effort to EUR 207 billion**.

The table below and the following charts depict the funding distribution across various instruments and Digital Decade targets.

Table 1. EU relevant budget for the Digital Decade targets (2021-2027 MFF, incl. RRF 2020-26, EUR million)

	Total	Recovery and Resilience Fund[226]	Cohesion Policy[227]	Horizon Europe	Digital Europe Programme	Connecting Europe Facility – Digital
Total budget	973 195	655 531	264 066	43 667	8 124[228]	1 806

[223] For all data reported in this paragraph, please see European Commission, 'Digital tracking', 2021.
[224] European Commission: Joint Research Centre, Nepelski, D. and Torrecillas, J., 'Mapping EU level funding instruments 2021-2027 to Digital Decade targets – 2025 update', Publications Office of the European Union, Luxembourg, 2025, JRC141966.
[225] The amount of funding considered under each programme and the distribution of funds across targets is strongly determined by the nature of the target and the assumptions made in the allocation.
[226] Including measures in the Repower EU chapters contributing to the digital transition. It should be noted that those measures are considered in the analysis in this report but do not contribute to the achievement of the 20% digital target set by the Regulation establishing the Recovery and Resilience Facility (see also the Guidance on Recovery and Resilience Plans in the context of REPowerEU). Data were extracted on 10 March 2025.
[227] While the overall Cohesion Policy funds total is EUR 392 billion, only the following funds are included in the mapping and subsequent estimations: the European Regional Development Fund (ERDF), the Cohesion Fund (CF), and the European Territorial Cooperation Fund (Interreg), including the digitalisation investments from the REPowerEU chapters.
[228] This amount is the sum of the planned budget per topic from all DIGITAL work programmes. It does not take into account the budget actually committed or the redistribution of available funds throughout the years.

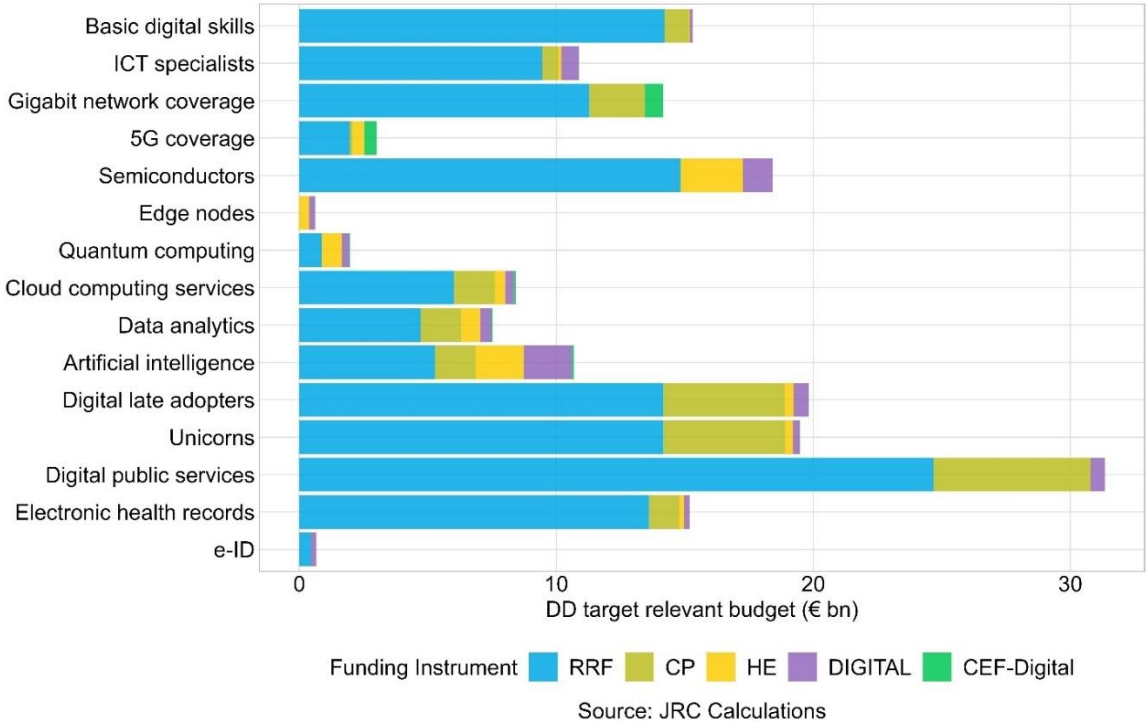
	Total	Recovery and Resilience Fund[226]	Cohesion Policy[227]	Horizon Europe	Digital Europe Programme	Connecting Europe Facility – Digital
Total Digital budget	207 067	149 813	29 594	17 730	8 124	1 806
Budget for other DD objectives	29 577	14 070	4 256	9 640	1 234	376
Total DD target-relevant budget	177 490	135 743	25 338	8 090	6 890	1 430
Basic digital skills	15 303	14 209	951	38	105	-
ICT specialists *	10 887	9 450	634	112	683	8
Gigabit network coverage	14 158	11 287	2 158	0	6	707
5G coverage *	3 010	1 967	115	446	6	476
Semiconductors *	18 423	14 836	-	2 426	1 161	-
Edge nodes *	621	-	-	390	224	7
Quantum computing *	1 982	878	-	789	279	36
Cloud computing services *	8 419	6 023	1 578	407	341	70
Data analytics *	7 514	4 722	1 578	745	420	50
Artificial intelligence *	10 684	5 282	1 578	1 876	1 870	78
Digital late adopters *	19 817	14 166	4 733	338	579	-
Unicorns *	19 481	14 170	4 733	306	271	-
Digital public services *	31 339	24 675	6 112	6	546	-
Electronic health records	15 184	13 610	1 168	201	205	-
eID	670	466	-	9	194	-

Note: The Digital Decade targets indicated in the table with an asterisk (*) benefit from HPC funding. This funding not only supports computing research and infrastructures (e.g. quantum, cloud, AI) but also the training of specialists, the development of hyper-connectivity (5G, edge nodes) and

semiconductors and the adoption of HPC or Big Data by SMEs. In total, HPC funding amounts to EUR 3.7 billion, channelled mainly through the EuroHPC Joint Undertaking (EUR 2.6 billion of the Digital Decade Target-relevant budget), RRF (EUR 950 million), DIGITAL (EUR 135 million) and Horizon Europe (EUR 9 million). Source: JRC calculations

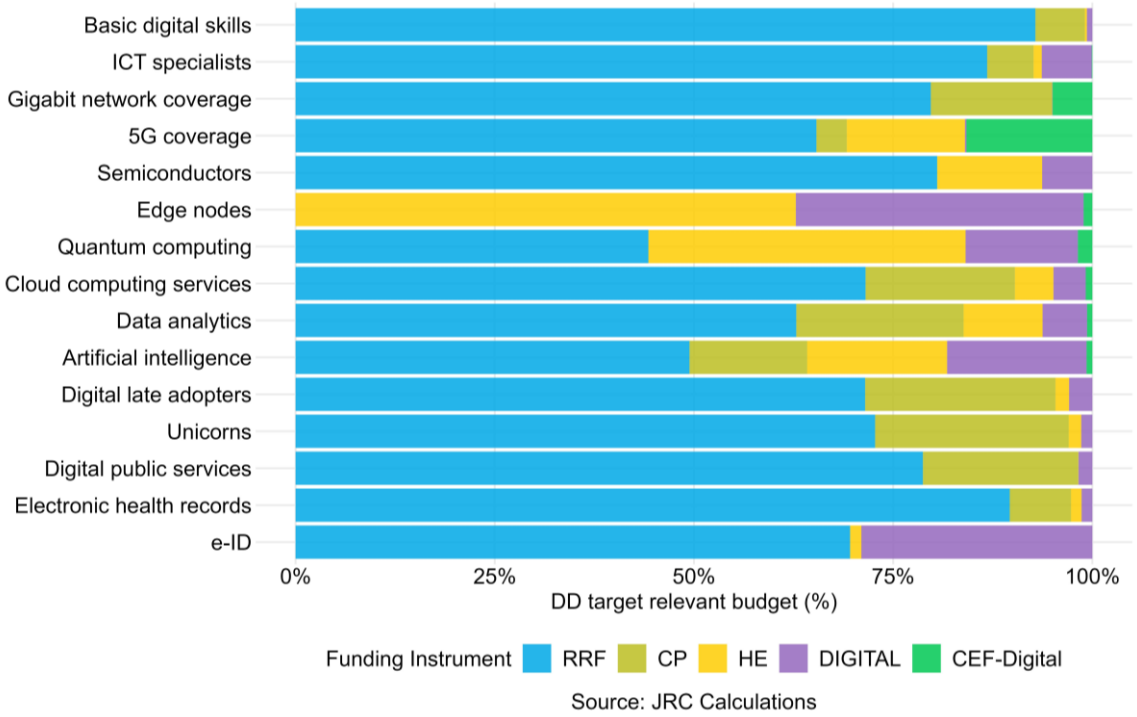
The following figures provide further visual representation of the support received by the different Digital Decade targets.

Figure 36. Digital Decade-relevant budget (billion EUR) by DD target



Source: JRC Calculations

Figure 37. Digital Decade-relevant budget (%) by DD target



Source: JRC Calculations

The **Recovery and Resilience Facility** (RRF) is the primary contributor, with EUR 149.8 billion dedicated to digital priorities, of which EUR 135.7 billion is considered to be contributing directly to the targets. This represents more than 70% of the total identified budget contributing to digital technology and to the targets specifically. The RRF plays an especially significant role in supporting basic digital skills (contributing to over 90% of the funding in this area) and ICT specialists (87%), as well in gigabit connectivity, digital public services, semiconductors, and e-Health (in all cases above 75%).

CEF Digital plays an important role in the development of the digital infrastructure, focusing on 5G, including cross-border backbones and stand-alone 5G for smart mobility, cities, and health.

The **Digital Europe Programme** significantly supports the deployment of AI, cloud computing, quantum, edge nodes, and eID, with a strategic focus on high-impact areas.

Horizon Europe is a key driver of digital innovation, covering especially advanced technologies such as quantum computing, edge, AI and semiconductors.

4.2.3 Investment needs for the digital transition

Estimates of the investment needs

There is a general consensus that a sharp increase in investment is essential for the EU to meet its strategic policy objectives in terms of competitiveness, digital leadership, and resilience. In recent years, several sector-specific analyses have been carried out to estimate specific investment needs. Although estimates vary and are subject to a certain degree of uncertainty and to an evolving landscape, they give important indications on the magnitude of the gaps.

The Draghi report estimates that there will be a need for an additional EUR **750-800 billion per year by 2030**, of which EUR 150 billion will be needed for 'becoming a leader in digital technologies' and EUR 100-150 billion for 'boosting productivity through breakthrough innovation'[229].

A recent study by the European Parliamentary Research Service (EPRS)[230] corroborates the magnitude of this gap. It estimates **investment needs per year** (more detailed indications are given by analysis estimating the gaps sector by sector) of between:

- EUR 55 billion and EUR 154 billion (of which public investment can be placed between EUR 10 billion and EUR 46 billion) for the EU to increase digital RDI spending and remain a leader on AI, quantum computing and other high-tech digital innovation (HTDI). These estimates draw on the gap with other economies like US and China, which is especially alarming in strategic sectors such as artificial intelligence, where the EU's share was at 10.2% in 2021, as opposed to China's 26% and the US's 29.6%.
- EUR 157 billion and EUR 227 billion (of which EUR 24 billion to EUR 68 billion of public investment) for additional annual investment in key digital technologies, skills, digital connectivity and infrastructure.

The box below offers an overview, drawing on the EIB Investment Report 2024/2025[231] and other sources.

Connectivity networks:

Substantial investments are needed in digital infrastructure to meet Europe's connectivity targets. According to the Commission's White Paper and underlying estimates[232]:

- EUR 148 billion is needed to achieve fixed Gigabit coverage using Fibre-to-the-Premises (FTTP), with EUR 43 billion requiring public funding.
- 'Full 5G'[233] deployment will require EUR 33.5 billion.
- Between EUR 26 billion and EUR 79 billion is needed for main transport corridor connectivity, depending on deployment options.

Overall, total digital infrastructure investment could reach EUR 200 billion by 2030, depending on the options considered (i.e. a combination of mobile, fixed wireless access (FWA), Fixed).

According to another study[234], achieving 91.5% FTTP coverage across the EU27 by 2030 would entail an additional cost of EUR 61.9 billion. An additional EUR 29.2 billion would be required to achieve 99% coverage. For 5G coverage using midband spectrum, a further EUR 25-30 billion is necessary.

Data centres for AI and cloud capacity

Investments needs in cloud computing and edge (data centres and the associated technology and service provision) are increasing quickly. Europe today has ca. 8-10 GW of installed data centre

[229] Draghi, M., 'The future of European competitiveness', 2024.
[230] EPRS, 'Benefit of an EU strategic innovation agenda – Cost of non-Europe', 2025. EPRS_STU(2025)762853.
[231] EIB, 'Investment Report 2024/2025: Innovation, integration and simplification in Europe', 2025.
[232] European Commission, White Paper - How to master Europe's digital infrastructure needs?, 2024, COM(2024) 81 final; M. Ockenfels, F. Eltges, T. Plueckebaum, I. Godlovitch, 'Investment and funding needs for the Digital Decade connectivity targets', 2023.
[233] Standalone 5G.
[234] Connect Europe, 'State of Digital Communications 2025', 2025.

capacity, amounting to roughly a third of the installed capacity in the US and half of the installed capacity of China[235]. According to industry, Europe's capacity will double by the end of the decade. Other forecasts indicate that Europe's capacity, as well as that of China, will grow by 70% between now and 2030. But despite these increases, due to Europe's low-capacity starting point, the gap with the US will continue to grow as the US is poised to increase its data centre capacity by 100%[236]. Some analysts and market research predict that demand for data centre services is expected to grow significantly in the next years, potentially widening Europe's computing capacity gap relative to global competitors[237]. Filling this gap will require significant investments.

Cybersecurity

A study from 2022 provides an extensive analysis of the investment landscape in cybersecurity in the EU and other major economies, and gives insights into the size of the gaps. It estimated that, in 2021, EU venture capital in the sector reached EUR 814 million – far behind the US (EUR 15 billion) and Israel (EUR 2.5 billion). Moreover, 70% of EU cybersecurity venture capital is concentrated in France, Germany, Italy, and Spain, with minimal cross-border investment, limiting the growth of larger funds[238].

Investment needs must be addressed by a combination of private and public funding, where the intensity of public support is likely to depend on the sector and the specific needs in terms of de-risking and incentives for private involvement.

In general terms and across all sectors, mobilising private funding and creating the right conditions has emerged as an imperative for EU competitiveness, sustainability and social and economic resilience.

In the EU, capital markets are underdeveloped. As recently highlighted by the ECB President, there are several barriers: a large share of European household savings is held in low-yield bank deposits rather than being invested in productive assets (entering capital markets); capital tends to remain within national markets, limiting cross-border investment flows and reducing the overall efficiency of capital allocation across the EU (expanding through Europe); the EU lacks a robust venture capital ecosystem, which means that innovative and high-growth companies – especially start-ups – struggle to access the financing they need (exiting into innovative sectors)[239].

Well-functioning capital markets are particularly crucial for investments in innovative technologies. There is a positive correlation between investment in innovative technologies and financial market development, explained by the important role played by market-based financing in supporting

[235] Hintemann, R., Hinterholzer, S., Progni, K., 'Data centres in Germany - Current market developments 2024', (2024a), Berlin: Bitkom e.V. Retrieved from Bitkom e.V. website..
[236] Ibid.
[237] The results of an ongoing study are expected to provide more granular data and empirical evidence to assess current and future needs of Cloud computing and Artificial Intelligence (AI) in the EU. The findings will enable the Commission to identify and quantify both existing capacity and future needs for general-purpose and AI-optimised infrastructure computing, also in terms of investment needs.
[238] EIB, European Commission, 'European Cybersecurity Investment Platform', 2022.
[239] Speech by Christine Lagarde, President of the ECB, at the 34th European Banking Congress: 'Out of the Comfort Zone: Europe and the New World Order', November 2024 (Follow the money: channelling savings into investment and innovation in Europe).

investments in high-risk, intangible and innovative assets that traditional bank financing might not adequately support[240]. Yet, compared to the US, EU start-ups and scale-ups face limited access to venture and risk capital. The EU accounts for only 5% of global venture capital fundraising, while the US attracts 52% and China 40%. This funding gap, combined with lower growth expectations and higher perceived risks for EU start-ups, diminishes their appeal to investors. As a result, many European innovators seek financing abroad – often relocating to the US to access broader markets and customer bases[241].

Leveraging the EU budget to support private investment, create synergies and maximise impacts

In this context, a substantial element is the need for the **EU budget to be better leveraged** to support private investment through different types of **financial instruments** and more **risk appetite**.

Joint Undertakings (JUs) and public private partnerships (PPPs) are geared to leverage and pool resources, in particular from industry. In the area of semiconductors, the Chips JU will raise EUR 11 billion in RDI investment by 2030. **However, the leveraging across partnerships and Joint Undertakings (JUs) is highly variable and not always sufficient[242]**.

EU financial instruments have a potentially high leveraging effect to attract private funds and investments. EU programmes' contributions could effectively be used as blending in combination with the InvestEU programme, to de-risk projects, stimulating private investments. **Nevertheless, financial instruments are not sufficiently mainstreamed in programmes[243] and still have limited investment portfolios composed mainly by demand and only indirectly by policy steer**. Depending on the level of technology readiness, **leveraging factors** from financial instruments are currently **around 3 for early-stage deep-tech** companies (European Innovation Council Fund equity) and **around 5.62 from the InvestEU guarantee**[244]. EU budgetary guarantees such as InvestEU have demonstrated advantages through **higher multiplier effects and the ability to support innovative projects**, such as deep-tech and critical technologies that may otherwise not be sufficiently funded by national schemes or that may not attract private capital due to the high risk involved.

The InvestEU programme

The InvestEU Programme is supporting digital investments and ecosystems across Europe through a combination of financing and advisory services. As per March 2025, investment supporting digitalisation amounts to **EUR 15.88 billion**. Of that amount, EUR **2.6 billion** correspond to financing and investment operations in digital connectivity infrastructure, technologies and services, resulting (amongst other impact indicators) in **2 120 000** additional households, enterprises or public buildings with broadband access of at least 100 Mbps upgradable to gigabit speed, or the number of Wi-Fi hotspots created.

Many of the digital transformation objectives under the InvestEU programme are closely aligned with

[240] EIB, 'Investment Report 2024/2025: Innovation, integration and simplification in Europe', 2025, pages 62-63.
[241] Competitiveness Compass for the EU, COM(2025) 30 final.
[242] Staff Working document (SWD) on Horizon Europe mid-term evaluation 2024
[243] As an example of the flexibility needed, 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 start-ups' (23 January 2024) | ScienceBusiness.
[244] European Commission, InvestEU interim evaluation, 2024, SWD(2024) 228 final.

the EU's digital targets for 2030:

- Strengthening Europe's presence in key parts of the digital supply chain (semiconductors, data technologies, 5G and quantum technologies which are of particular importance for security and strategic autonomy).
- Supporting digital transformation ecosystems and businesses by equipping them with the necessary digital tools.
- Improving connectivity and bandwidth to ensure appropriate services for health, education, transport, logistics and media as well as reducing the geographical digital divide.
- Driving investments in audiovisual and media domains essential for democracy and cultural diversity, particularly in innovative media content and technologies, to improve long-term capacity to produce and distribute content and to compete globally in such areas.
- Contributing to a sustainable, climate-neutral and resource-efficient economy through digital investments and green digital technologies.
- Developing and deploying digital technologies such as supercomputing, artificial intelligence, blockchain, cloud data, and Internet of Things.

Overall, EU financial instruments and budgetary guarantees have a strong potential to catalyse private investment – particularly in high-risk, high-impact areas such as deep-tech – and are effective in scaling up innovation and supporting market-driven projects. Other aspects of the digital transition, however, require sustained public investment and targeted policy action, for example when it comes to promoting an inclusive digital transition, monitoring of digital inequalities, and tailored support for vulnerable populations. This also holds true at local level, with many municipalities lacking the necessary financial and human resources to implement effective digital inclusion strategies or assess local needs through data-driven approaches[245].

Another crucial aspect is ensuring **an impactful EU budget and coordinated action across the EU**. The 2024 State of the Digital Decade report called for stronger collaboration between Member States and the European Commission to enhance synergies across EU funding programmes and to focus on high-impact projects, geared towards common objectives and with a strong cross-border dimension to pool resources and help accelerate progress toward the Digital Decade objectives.

Initiatives like **EDICs, IPCEIs, and Joint Undertakings** are proving essential in coordinating multiple funding sources and pooling resources, becoming scalable models for coordination. However, in general terms, the **practical implementation of synergies across programmes remains complex**, particularly for SMEs lacking the resources to navigate opportunities effectively.

There is also room to **tailor funding programmes more closely to the EU priorities**. For example, a recent European Court of Auditors report on the contribution of the Recovery and Resilience Facility to the digital transition recommended to strengthen the link between EU funding schemes and the main digital needs identified. The Court recommendation requires the Commission to 'target the allocation of funding more effectively, such as by requiring a clear link to the EU's digital transition

[245] Eurocities, 'Digital Divide Observatories by European cities', 2022.

strategy and prioritising the funding of the previously identified digital needs'[246]. These conclusions will be used, in particular, in the preparation of the next multiannual financial framework.

Addressing these issues is at the core of recent policy action, starting from the Competitiveness Compass[247] and its proposed competitiveness tool, and the Communication on the next long-term EU budget, which calls for 'strong mechanisms … to guarantee that the funds deliver on EU policy priorities'[248].

4.3 Cooperation with cities and regions as a tool for implementing and disseminating digital policy

To meet the demographic challenges facing our workforce and preserve our prosperity, the European Union faces a critical challenge: ensuring that digitalisation drives productivity. In the context of the Digital Decade, the digitalisation of businesses, particularly SMEs, is central to this effort. However, one of the key issues highlighted by the **State of the Digital Decade 2024 report** – **the dissemination of digital technologies** – remains uneven.

While metropolitan areas often act as innovation hubs, many regions lag behind, creating a digital divide that hinders Europe's overall competitiveness. Strengthening cooperation between the Commission, Member States, and their cities, especially from innovation hotspots to smaller cities, can play a crucial role in addressing this gap. By enabling **technology spillovers**, cities can thus help disseminate digital tools to businesses across all regions, enhancing productivity and resilience. Beyond their role in such dissemination, cities are also at the heart of ecosystems that merge **technology, sustainability, and European values**. Smart urban planning allows cities to integrate green initiatives – such as sustainable transport and clean energy networks – with digital innovation, creating environments that safeguard democracy, protect privacy, and enhance the well-being of residents. Thus, **as cities are the closest level of public administration to citizens** and have a particularly good understanding of the needs and constraints of their residents and SMEs, **placing a focus on them is a great opportunity for the EU to tackle the priorities of the new Commission.**

In this context, **the Commission is planning to put forward an ambitious policy agenda for cities.** This agenda, for which Executive Vice-President Raffaele Fitto is responsible, should provide a clear vision for the future of the cities, looking at issues such as housing, climate action, mobility, social inclusion, equality, mobility and digitalisation[249]. Within this framework, the Digital Decade Policy Programme presents a valuable opportunity to provide guidance and support for shaping this agenda for future cities, promoting key priorities for action and various tools.

4.3.1 The need for data to monitor public policies

First, in order to drive effective digital transformation and ensure data-driven policy, improving measurement tools is essential in the context of the Digital Decade 2030, building on **local initiatives, such as the Living-in-EU movement and the LORDIMAS tool.** Such monitoring plays a crucial role in

[246] ECA, 'Support from the Recovery and Resilience Facility for the digital transition in EU member states, A missed opportunity for strategic focus in addressing digital needs', 2025.
[247] Competitiveness Compass for the EU, COM(2025) 30 final.
[248] The road to the next multiannual financial framework, COM(2025) 46 final.
[249] European Commission, Raffaele Fitto - Mission Letter, 2024

tracking digital maturity at the regional level, enabling policymakers to adapt their strategies to the needs of each area.

To understand the complexity behind the interplays between EU policy objectives and the realities and the context on the ground, we need data. However, there are very few harmonised and comparable indicators being collected or produced that cover the local level across the bloc. Much of the current monitoring of digital transformation is carried out only at regional or national level. A strategic and targeted approach to monitor and measure what is happening at local and regional levels is still largely missing. This first report on LORDIMAS seeks to partially address this knowledge gap by utilising LORDIMAS data to provide insight into the state of digital maturity of subnational public administrations. 2024 was the first full year of LORDIMAS data collection, encompassing data from approximately one hundred local, metropolitan, and regional governments. It features an analysis of digital maturity based on the LORDIMAS self-assessments conducted in 2024 by 99 local, metropolitan and regional authorities.

To enhance the representativeness of data and strengthen the evidence base for European policymaking, LORDIMAS aims to increase the number of participating administrations year-on-year. The number of participating local and regional administrations continues to rise in line with ongoing outreach campaigns (status 30 March 2025: 184 entries).

Developing digital twins, in particular through the LDT-CitiVERSE-EDIC, provides cities with a common EU-wide digital infrastructure including powerful tools for key urban challenges (e.g. urban development, Net Zero Cities, New European Bauhaus (NEB) implementation) under the first SIMPL-based EU Data Space. This EDIC**,** set up by a Commission Decision in February 2024**,** was officially launched in Valencia, Spain, in December 2024. **It aims to establish a shared EU-wide infrastructure for data and services**, to be used by the 100 cities expected to join the CitiVERSE EDIC during 2025. The project then aims to establish **EDIC joint agreements** with relevant players, such as the European Digital Innovation Hubs (which will receive funding in 2025 for developing their data strategies), Scalable Cities, and the NEB hubs that will empower this EDIC with other very important EU-funded results and facilitate the process of scaling up the digital EU Cities ecosystem.

In the future, EU cities participating in EDIHs, Scalable cities and AI-based twinning (through HPC) could develop **more advanced Local Observatories, building on the experience of similar existing Observatories**, to monitor digital transformation and efficiently allocate resources (including emergency response and urban resilience under NEB principles) and measure progress toward the Digital Decade objectives.

Regarding Digital Capacity Building for cities, the **LDT-CitiVERSE-EDIC** will develop a new node for the New European Bauhaus Academy facilitating technical support for the creation of new SMEs supporting the digital component of the EU Cities ecosystem.

4.3.2 Building comprehensive and resilient digital ecosystems

Resilient digital transformation relies on robust ecosystems that integrate skills development, connectivity infrastructure, and enterprises' support, especially for SMEs. In 2023, only 55.6% of Europeans possessed basic digital skills, with significant disparities between urban and rural areas (63% of people living in cities compared with 48% of people living in rural areas) and a gender gap in digital professions. To address these discrepancies, it is crucial to enhance ICT specialist training and encourage digital skills development from an early age, particularly by motivating young people, especially girls, to enter STEM fields.

SMEs need resources to adopt advanced technologies (AI, cloud, IoT), which strengthens their competitiveness and supports an inclusive digital economy. Actions encouraging SMEs to adopt advanced technologies, such as AI, IoT, and cloud computing, should therefore be explored, with assistance in assessing needs, implementing solutions, and navigating EU funding opportunities. A good way forward to promote the dissemination of technologies would also be to **streamline procedures for accessing EU funding,** particularly for smaller municipalities and SMEs.

European Digital Innovation Hubs (EDIHs) are instrumental in advancing digital transformation within cities across Europe by providing essential services such as **training, testing facilities, and partnerships** with technology providers. For example, the majority of EDIHs are actively collaborating with cities to implement smart-city projects and facilitate the testing and deployment of digital solutions.

The **AI Testing and Experimentation Facilities (TEFs)** are large-scale reference sites that allow technology providers across Europe to test advanced AI solutions in real-world settings. **CitCom.ai**, the TEF focused on **smart cities and communities**, targets sectors like **energy, mobility, and connectivity**, aiming to test AI and robotics before they are deployed in public spaces. This includes technologies such as self-driving vehicles and telecom data software. CitCom.ai functions as a bridge between technologies, infrastructure, and everyday life, with **three super nodes** (Nordic, Central, South) and **satellites across 11 EU countries**. Co-funded by the **Digital Europe Programme**, this EUR 40 million project began in **January 2025.**

It is also fundamental to **prioritise investment in the Digital Decade connectivity targets, e.g. for high-speed internet, in particular 5G and fibre** for underserved areas, ensuring that all cities, regardless of their size, have the infrastructure to support digital innovation. **Funding pilot projects** in smaller cities is also a priority to demonstrate the benefits of digital technologies in urban management.

Reinforcing sovereign and secure public digital services within cities is essential to ensure access to quality services and to protect European technological autonomy. In this regard, the Connecting Europe Facility (CEF) Digital programme plays a key role in supporting and catalysing investments in digital connectivity infrastructure. Among its actions, CEF Digital co-finances projects such as 5G for Smart Communities, which funds rapid deployment and uptake of 5G for smart communities and innovative applications. EUR 128 million has already been committed to finance 41 projects advancing 5G connectivity, smart infrastructure, and digital transformation across Europe, including municipality-led projects such as High Connectivity via 5G in Toulouse, France (EUR 2.8 million), enhancing smart traffic management and surveillance, and 5G4LIVES in Riga, Latvia, and Turin, Italy (EUR 2.9 million), focusing on emergency risk prevention and disaster management. The CEF Telecom programme facilitates cross-border interactions between public administrations, businesses, and citizens, deploying digital service infrastructures and broadband networks. Additionally, WiFi4EU has supported more than 7 200 European municipalities in installing over 93 000 free public Wi-Fi hotspots, making digital access more inclusive for local communities.

4.3.3 Anchoring actions to digital rights and principles

Cities are essential actors in **implementing the DDPP-monitored European Declaration on Digital Rights and Principles,** which offers a framework to ensure that the digital transition is ethical, inclusive, and respectful of fundamental freedoms.

The Commission's monitoring of digital rights and principles aims, in particular, to pay closer attention to the initiatives of cities and local actors, and emphasise their role in the promotion of digital rights.

In addition, **local actions, such as the Brussels Digital Rights Charter or Leipzig's Hardware for Future** initiative, actively contribute to strengthening digital inclusion and equitable access to technology. The DDPP works **in partnership with the Cities Coalition for Digital Rights**, supporting initiatives across the EU, and serves as a model for local mobilisation in favour of digital rights, reinforcing public trust and protection in digital services. The local level also presents opportunities to promote key technology regulations, such as the AI Act, the DSA and the DMA, among the public.

The 2025 Eurocities Digital Forum: Digital Rights at the Heart of Cities, hosted by Bordeaux Métropole at the beginning of April, brought together city leaders and experts to shape digital innovation in inclusion, dignity, and democratic resilience. Amid rising concerns over AI, misinformation, and shrinking civic space, cities reaffirmed their role as defenders of democratic values, calling for stronger EU-local cooperation and people-centred digital policies.

4.3.4 Launching (or building on existing) concrete cooperations at EU level

The landscape where EU policies and initiatives will have to have an impact is fragmented, complex and diverse. There are approximately 90 000 local and 250 regional governments in the EU and EFTA countries, each tasked with providing similar services and support to the public, and each with their own – largely duplicated – digital infrastructure and processes. Hence, digital transformation necessitates strong cooperation between public administrations to achieve scalability, interoperability, and cost-effectiveness. **Collaboration is essential** for optimising resource utilisation, facilitating the sharing of knowledge and best practice and promoting the seamless exchange of digital infrastructure and services. **By working together, public administrations can avoid the inefficiencies and costs** associated with duplicating efforts or reinventing solutions that already exist elsewhere.

Succeeding in the digital and ecological transitions must rely on strong cooperation between cities, Member States, and the Commission. Designated programmes like the DDPP's EDIC CitiVERSE consortium, but also the New European Bauhaus, Digital Innovation Hubs (EDIHs) and the European Smart Communities Data Space, will provide additional resources and platforms for cities and regions to drive environmentally focused digital transformation efforts.

The **EU Cohesion Policy Fund** and the **European Urban Initiative**, launched in 2023, support the development of inclusive and sustainable digital services, especially in regions with limited private investment.

The Commission seeks to maximise the impact of local initiatives by strengthening cross-border collaboration and encouraging the sharing of best practices, as on the **Digital Skills and Job Platform**. The suggestion proposed by the Cities Coalition for Digital Rights to establish EU-funded city consortia for the dissemination of good practices to combat digital inequalities could be explored. Mapping local initiatives through observatories provides a baseline for monitoring progress and would allow regional and national actions to be aligned more closely with the EU digital strategy.

Moreover, the **Horizon Europe Mission on Cities (Cities Mission)** is another ongoing leading EU initiative on the digital and ecological transitions, with a strong engagement of cities. It involves local authorities, the public, businesses, investors as well as regional and national authorities to deliver

100 climate-neutral and smart cities by 2030 and to ensure that these cities act as experimentation and innovation hubs to enable all European cities to follow suit by 2050.

As set out in its implementation plan, the Cities Mission takes a cross-sectoral and demand-led approach, creating synergies between existing initiatives and basing its activities on the actual needs of cities.

Combining efforts at all levels can build a truly human-centred and sustainable digital society. The DDPP aims to foster multiscale cooperation, in consultation with all stakeholders.

Best practice: Portugal – Smart Territories National Strategy (ENTI)

Launched in August 2024, Portugal's Smart Territories National Strategy (ENTI) presents a comprehensive approach to transforming territorial governance through data-driven innovation. Anchored in sustainability, transparency, and interoperability, the strategy fosters more efficient public service delivery and supports climate resilience by integrating digital tools such as digital twins, policy dashboards, and urban management platforms. Funded by the Recovery and Resilience Facility with a budget of EUR 60 million, ENTI promotes collaborative innovation across municipalities and sectors, enhancing the use of real-time data for decision-making. Key success factors include improved regional development, digital inclusion, and smarter infrastructure planning, particularly in addressing urban-rural disparities. The strategy aligns with EU digital rights and principles by prioritising inclusivity, environmental monitoring with the deployment of smart grids, and 5G connectivity. It offers a scalable model for Member States seeking to enable smart, green, and connected territories through coherent national action.

4.4 The international dimension of the Digital Decade

International aspects of digital policies are intrinsically linked to internal ones. Building on the EU's strengths and internal policies and actions, the International Digital Strategy for the European Union[250] seeks to (i) boost the EU's tech competitiveness through economic and business cooperation with trusted partners (ii) promote a high level of security for the EU and its partners and (iii) shape global digital governance and standards in line with the EU values-based approach.

To safeguard economic interests, 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 increase the EU's resilience in critical sectors.

Instruments like the European Declaration on Digital Rights and Principles have influenced international agreements such as the OECD's Declaration on a Trusted, Sustainable and Inclusive Digital Future and discussions for a UN Global Digital Compact. The EU has laid the foundations for digital diplomacy through Council Conclusions[251], and aims for a stronger, more strategic and

[250] An International Digital Strategy for the European Union, JOIN(2025) 140 final.
[251] Council Conclusions on EU digital diplomacy of 18 July 2022 and 26 June 2023, and Council Conclusions of 18 April 2024 which further emphasised the importance if the international dimension of EU digital policies.

coordinated approach to digital coalition building and diplomatic outreach, allowing the EU to lead the way in global digital governance.

The international dimension of digital policies is closely intertwined with the EU's internal regulatory framework. A key aspect of international cooperation in this field is the promotion of the EU's digital standards beyond its borders. In this context, the EU is actively working to extend the Roam-Like-At-Home (RLAH) Regulation to candidate countries such as Moldova.

The EU has developed **international digital partnerships**, building on our strong ties with like-minded partners. Such partnerships are structured across **three levels:**

1. Trade and Technology Councils, Digital Partnerships and Digital Trade Agreements
2. Digital Dialogues
3. Partners we cooperate with through the Neighbourhood Policy, Global Gateway and regional alliances

The EU's international digital partnerships correspond to the four pillars of the Digital Compass – skills, infrastructure, transformation of business and transformation of public services – and build on a 'cooperation toolbox' including regulatory cooperation, RDI and industrial cooperation, investment in secure digital infrastructure, capacity building and skills and cooperation in international forums.

4.4.1 Trade and Technology Councils (TTCs), digital partnerships and digital trade agreements

The Commission has continued to develop its network of international digital partnerships, developing cooperation on research collaboration, regulatory policy and standardisation.

The EU has discussed cooperation in key areas such as artificial intelligence, emerging technologies, secure and resilient connectivity at the sixth EU-US TTC ministerial meeting which took place on 4-5 April 2024 in Leuven, Belgium[252].

During the 2nd TTC meeting with India, held on the margins of the unprecedented College visit to India in February 2025, both India and the European Union reaffirmed the importance of deepening their digital cooperation in line with their shared values through the TTC Working Group 1 on Strategic Technologies, Digital Governance, and Digital Connectivity.

The European Union is committed to advancing the common tech agenda with India, with a focus on key digital technologies such as artificial intelligence, semiconductors, digital public infrastructure, 5G/6G and high-performance computing, as well as facilitating the exchange of skilled professionals and talent.

Over the course of 2022, **three digital partnerships with key East Asian countries – Japan, South Korea and Singapore – were launched. These partnerships showcase the EU's strategic engagement in the digital field with this pivotal region of the world.** They aim to provide an overall framework for bilateral cooperation on (i) digital policy and regulatory matters (such as data free flow with trust, online platforms, cybersecurity and AI), (ii) our positions on digital matters in international forums and (iii) research and investment opportunities in cutting-edge technologies such as HPC,

[252] Sixth EU-US TTC Ministerial meeting, 'EU and US continue strong trade and technology cooperation at a time of global challenges', 2024.

semiconductors and 5G/6G. In 2024, Digital Partnership Councils were held with both Japan and the Republic of Korea to further cooperation on AI, semiconductors, 5G/6G, digital identities and trust services, quantum and high-performance computing, Arctic connectivity, data governance, online platforms and cybersecurity.

The EU has launched new joint projects with its partners to reinforce mutual economic resilience, increase the EU's excellence in RDI and boost competitiveness. A key project is to deploy a secure and direct submarine cable between the EU and Japan and the rest of the region through the Arctic.

Following the successful start of the partnerships in East Asia, the EU launched a digital partnership with Canada on 24 November 2023 on the occasion of the EU-Canada summit. It covers issues such as AI, quantum computing, cybersecurity, digital identities, arctic connectivity and online platforms. The Partnership was implemented in 2024 through expert exchanges.

The EU also already has a growing portfolio of free trade agreements[253] and digital trade agreements[254], which was expanded most recently with agreements with Japan, Singapore and the Republic of Korea, which set high-standard digital trade rules in line with EU-values that ensure a secure and safe online environment for consumers, bring transparency, predictability and legal certainty for companies, and prevent or remove unjustified barriers to digital trade including for cross-border data flows.

4.4.2 Digital dialogues

The EU's international digital partnerships are underpinned by a growing programme of bilateral digital dialogues with key partners around the world.

In the **Latin America and Caribbean (LAC)** region, bilateral digital policy dialogues have been set up with **Brazil** (which took place on 12 February 2025), **Argentina** (which took place on 21-22 June 2023) **and Mexico**. These are complemented with bi-regional policy dialogues established under the EU-LAC Digital Alliance on: Data governance, cybersecurity, e-governance, connectivity and inclusion, artificial intelligence.

In **Asia**, the EU held a second High Level Dialogue on Digital with **China** on 18 September 2023. The dialogue addressed problems EU companies encounter in China, such as access to ICT standardisation bodies, and cross-border data flows. Further to that, a China-EU ICT Dialogue took place on 29 February 2024.

The Digital Dialogue with Australia was successfully relaunched on 12 June 2024 following a four years pause. The Dialogue included exchanges on AI, data economy, cybersecurity and agreed on increased and systematic cooperation on platforms.

4.4.3 Global Gateway and regional alliances

The programme of policy dialogues is accompanied by a growing number of digital cooperation initiatives, supported by instruments such as NDICI-Global Europe, the Connecting Europe Facility and Horizon Europe, in addition to Team Europe initiatives which bring together the contributions of Member States.

---

[253] EU Trade agreements, European Union.
[254] Digital Trade Agreements, European Union.

The Global Gateway initiative focuses on digital infrastructure investment to bridge the global digital divide and increase the security of digital connections between Europe and its partners. The Commission is in particular supporting the deployment of secure 5G networks provided by trusted vendors in non-EU countries, notably in the LAC region and the EU neighbourhood. It is also working on supporting the security and resilience of submarine cables, supporting the EU's digital resilience and reducing dependencies.

To promote a 'Team Europe' approach, the Commission and Member States joined forces to implement a coordination platform aimed at strengthening the EU's global role in support of a human-centric model of digital transformation: the D4D Hub.

4.4.4 Candidate countries

The Commission has supported digital transformation efforts in enlargement countries and the EU neighbourhood, including by granting them the status of association with EU programmes like Digital Europe and the Connecting Europe Facility. Association agreements to the Digital Europe programme were signed with Montenegro and Türkiye.

The Commission held its third Regulatory Dialogue on digital policies with **Western Balkans countries** on 18 October 2024 in Brussels. The Dialogue focused on issues such as AI, the DSA and DMA, cybersecurity (including the 5G cybersecurity toolbox) and digital identity.

Since the start of Russia's invasion of **Ukraine**, the EU has substantially stepped up support for the country's digital transformation, focusing both on emergency and long-term measures. The voluntary agreement between several EU telecom operators and Ukraine's operators to ensure affordable connectivity for Ukrainian refugees has been extended for a fifth time until 9 July 2025. At the same time, the EU has continued to work, through the EU-Ukraine Association Agreement, towards a long-term roaming arrangement with Ukraine. The third EU-Ukraine cyber dialogue took place on 15 July 2024. In December 2024, Ukraine formally expressed its interest in participating in the EU Cybersecurity Reserve. In the same month, the amendment of Ukraine's Association Agreement to Creative Europe was signed to allow Ukraine to participate in all the actions of the MEDIA strand of the programme.

A similar approach for roaming is being followed with **Moldova**, where efforts towards a long-term arrangement through the EU-Moldova Association Agreement are being complemented by a short- to medium-term voluntary agreement between operators on both sides. The EU has supported Moldova by ensuring the integrity of the country's Presidential elections, which took place in October 2024.

Between March and December 2024, the Commission and **Switzerland** negotiated on a broad package of agreements to deepen and expand the EU-Switzerland relations. The conclusion of negotiations was announced by Commission President von der Leyen and Swiss President Amherd on 20 December 2024. The outcome of the negotiation fulfils the Council mandate and reflects the balance described in the Common Understanding, a political document in which the Commission and Switzerland mapped out the overall package and landing zones. The package includes an agreement on Switzerland's regular and fair financial contribution to the EU's cohesion, as well as an agreement on Switzerland's association to EU programmes (e.g. Horizon Europe, Digital Europe, ITER, Erasmus+).

4.4.5 Multilateral cooperation

The EU has recorded significant success in multilateral forums.

In 2023, **G7** Leaders endorsed a voluntary code of conduct for AI developers, drawing upon key concepts from the EU AI Act. This initiative was further strengthened in 2024 when OECD countries also endorsed the Code. To put the Code into practice, a monitoring mechanism and a logo were developed. The Commission continues to play a pivotal leadership role on the multilateral front, actively promoting the 'Data Free Flow with Trust' initiative, which reflects the idea (at the heart of the EU data regulations) that data protection is not a 'restriction' but an enabler to data flows, which increases trust in the digital economy. This is shaping the G7/20 discussions and supports the work of the OECD.

In the **OECD,** the Commission is proactively promoting the EU model for the digital transformation. The EU brought to conclusion the discussions on the first-ever international instrument setting out principles in the area of surveillance, the Declaration on Government Access to Personal Data Held by Private Sector Entities. The OECD also adopted the OECD AI principles and 28 countries joined its Global Partnership on AI (GPAI). In the area of data free flow with trust, the EU successfully supported the Japanese proposal to set up a forum at the OECD called the Institutional Arrangement for Partnerships, dedicated to exchange, among like-minded countries.

At the **WTO,** the EU contributed to the successful renewal of the Work Programme on electronic commerce and the moratorium on customs duties on electronic transmissions at the 13th Ministerial Conference in February 2024 for a further two years, ensuring that the duty-free digital environment that has been in place since 1998 was maintained. The EU also played a major role in the negotiations for a plurilateral eCommerce Agreement that concluded in July 2024. Once integrated into the WTO, the eCommerce Agreement will be the basis for global rules on digital trade among a broad range of WTO Members.

In the **UN** context, the EU contributed to an ambitious **Global Digital Compact (GDC)**, which is the first comprehensive framework for global digital governance. The GDC largely reflects EU priorities on how to reconcile human rights, democracy and the rule of law in this new area of digital governance, in line with the European Declaration on Digital Rights and Principles and the human rights conventions, covenants, and treaties.