EUROPEAN COMMISSION

Brussels, 16.6.2025
SWD(2025) 293 final

COMMISSION STAFF WORKING DOCUMENT

Monitoring of the European Declaration on Digital Rights and Principles

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

EN
EN

Monitoring of the European Declaration on Digital Rights and Principles

2025

Contents

Introduction

The <u>European Declaration on Digital Rights and Principles for the Digital Decade</u> sets out a vision and concrete commitments for how rights and freedoms enshrined in the EU's legal framework as well as European values translate into a digitally transformed world. Signed in December 2022, the Declaration aims to give everyone a clear reference point for the type of digital transformation the EU wants. It also provides a guide for policymakers and businesses when dealing with digital technologies, measures, and policies.

As explained in the Declaration, the EU wants to secure European values by (i) putting people at the centre of the digital transformation; (ii) supporting solidarity and inclusion through connectivity, digital education, training and skills, fair and just working conditions and access to digital public services; (iii) ensuring freedom of choice and a fair digital environment; (iv) fostering participation in the digital public space; (v) increasing safety, security and empowerment online, in particular for young people; and (vi) promoting sustainability.

While the Declaration has a declaratory nature and, as such, does not affect the content of legal rules or their application, its political importance should be acknowledged. Signed at the highest level of the EU, the signatories have acknowledged that its promotion and implementation are a shared commitment and responsibility of both the EU and its Member States. In the same spirit, the Digital Decade Policy Programme provides that Member States and the Commission must take into account the digital rights and principles in the Declaration when cooperating to achieve the general objectives of the Digital Decade Policy Programme.

This Commission staff working document presents actions taken in relation to the digital rights and principles at both European and national level, making a connection between the Declaration's concrete commitments and the initiatives that have been adopted. The document adopts a positive approach. Using examples and best practices from across the EU, it illustrates possible ways to promote and apply digital rights and principles in order to inspire further policy action and outreach on this topic. The document also complements the analysis on the progress towards the EU's Digital Decade targets and objectives presented in the 2025 State of the Digital Decade Report.

Methodology

The Commission has committed to regularly report to the European Parliament and the Council on the progress made in promoting and implementing the Declaration. This edition builds on 2023 and 2024 monitoring reports and aims to provide an overview of the implementation of digital rights and principles, focusing on initiatives adopted by the end of 2024. The findings provide an overview of action at both the EU level and national level, drawing on various sources. These sources include (i) an independent study[1] commissioned by the Commission, collecting further contributions from Member States, industry and civil society; (ii) the Digital Economy and Society Index (DESI); (iii) stakeholder input, including from Member

---

[1] Study to support the monitoring of the Declaration on Digital Rights and Principles, available here: <u>https://digital-strategy.ec.europa.eu/en/news-redirect/883230</u>

States; and (iv) various Commission and other reporting mechanisms. Moreover, the 2025 Special Eurobarometer Report on the Digital Decade[2] gives an insight into people's perceptions on digital rights and principles.

The 2024 monitoring report highlighted Members States' good practices to inspire further action across the EU. This editions' focus goes beyond highlighting good practices by making a more quantitative assessment of the application of digital rights initiatives across the EU. For this purpose, the independent support study developed an impact indicator framework to illustrate the level of implementation of digital rights initiatives on the ground.

The impact indicator framework estimates the impact of digital rights initiatives implemented by key stakeholders in Member States (mainly national governments). The framework takes into account available data across EU-27 (such as DESI) or data reported by Member States (such as from the Berlin Declaration Monitoring 2024). It also looks at how people perceive these measures, mainly through Eurobarometer data. Currently, around two thirds of the 51 Declaration commitments are covered by the indicators.

As an illustration, indicators with EU-27 data are available for 12 out of 17 commitments under the *Solidarity and inclusion* Chapter *(Chapter II)*. Such data include quantitative and qualitative data from DESI, the Berlin Declaration Monitoring Mechanism, the eGovernment Benchmark, the International Computer and Information Literacy Study, as well as people's perceptions collected via the Special Eurobarometer Survey on the Digital Decade, and Eurostat[3].

While this impact indicator framework provides a basis for future monitoring and identifying trends, it is based on available data that is not always consistent. More comprehensive and systematic data from Member States and stakeholders would be useful. More generally, the support study also includes a number of recommendations to address the gaps identified for further reporting.

The support study is also accompanied by visual country factsheets, including country-specific analysis of digital rights initiatives, their estimated impact, areas with most activity, gaps and recommendations. These have also served as an important source to monitor digital rights and principles in the 2025 Digital Decade country reports.

Executive summary

The European Declaration on Digital Rights and Principles offers citizens a bridge to Union digital laws and policies, as it indicates the EU's direction of travel towards digital transformation. This document aims to show to what extent the EU and its Member States are following that trajectory.

---

[2] 2025 Special Eurobarometer Report on the Digital Decade, available here: https://digital-strategy.ec.europa.eu/en/news-redirect/883227
[3] The full list of indicators is published in an annex to the support study, available here: https://digital-strategy.ec.europa.eu/en/news-redirect/883230

EU action

In 2024 the EU has continued to be very active in promoting and applying the human centric and fundamental rights-based approach to digital transformation as outlined in the Declaration. This is for instance demonstrated in the adoption of the Artificial Intelligence (AI) Act, which aims explicitly to promote the uptake of human centric and trustworthy artificial intelligence while ensuring a high level of protection of health, safety, fundamental rights. The bans on AI systems that do not comply with fundamental rights started to apply in February 2025. Also, the EU adopted a Regulation establishing the European Digital Identity Framework, which will offer all EU citizens the possibility to have an EU Digital Identity Wallet to access public and private online services in a secure way while protecting their personal data across the EU. And the European Media Freedom Act (EMFA) has been adopted, which puts in place a new set of rules to protect media pluralism and independence in the EU.

Moreover, in 2024, the Commission worked tirelessly to implement and enforce its landmark digital rules. For instance, this included enforcing the Digital Services Act and of the Digital Markets Act, which contribute to ensuring respect for fundamental rights in the digital environment. For instance, the Commission has opened a number of formal proceedings against the providers of the very large online platforms because of potential breaches of the DSA, including in respect of obligations with regard to the spread of illegal content and disinformation or in respect of minor protection online.

Building on its recent and comprehensive digital rulebook, the EU has been promoting its human-centric vision of digital transformation on the global stage, both at multilateral and bilateral level. At multilateral level, the Declaration provided a strong basis for the United Nations Global Digital Compact, the first comprehensive framework for global digital governance agreed at the Summit of the Future in September 2024.

At this point in time, it should be noted that the human-centric vision of digital transformation continues to underpin the Commission's work for 2024-2029, as is clear from the Commission Work Programme 2025 that was adopted in early 2025.

Citizens' perceptions

European citizens need to know their rights if they are to exercise them. According to the 2025 Special Eurobarometer Survey[4], **Europeans' awareness of their digital rights has however not increased in recent years** (standing at 59%, slightly lower than the 2024 rate of 62%). And only 44% feel well protected in the digital space (similarly to 45% in 2024). It is also worth noting that the survey results differ by Member State, sometimes significantly, as illustrated later on in this document.

At the same time, **when looking at specific rights and principles surveyed, the outlook seems relatively more positive**. A significant majority (60%) of Europeans feel that they are getting the necessary basic or advanced digital education, training and skills. Also, a stable majority continues to think that the freedom of expression and information online, e.g. via online platforms, social networks or search engines, is well protected in their country (60%, similarly to previous years), as well as their right to freedom of assembly and association in the digital environment (59%, similarly to previous years). Moreover, 57% of Europeans

---

[4] The 2025 Special Eurobarometer Report on the Digital Decade, available here: https://digital-strategy.ec.europa.eu/en/news-redirect/883227

consider that they have access to an affordable high-speed internet connection (57% in 2024, 53% in 2023), and 58% (as in 2024) find it easy to access digital public services.

Still, most Europeans (55%) consider that they have access to safe and privacy-friendly digital technologies in their country. Slightly fewer Europeans (54%) think that people working in the digital environment are benefiting from fair and healthy working conditions, including work-life balance. Over half of Europeans (53%) believe that they have access to a trustworthy, diverse and multilingual digital environment, including more diverse content, less disinformation, and less illegal content. And 53% of Europeans believes that they are getting effective freedom of choice online (compared to 52% in 2024 and 49% in 2023), including when interacting with AI (e.g. chatbots, digital assistants).

Nevertheless, in keeping with the principle of an inclusive digital transformation and noting the absence of progress over the last year in the above domains, **one should not be satisfied that one third or sometimes more Europeans find that digital rights and principles are not well applied in their country**.

Moreover, other areas are perceived less positively. Only half of Europeans (50%, same as last year) consider that they have access to digital products and services that minimise damage to the environment and society. This includes products and services that can be repaired or recycled, and which do not involve forced labour. Similarly, 49% (comparable to last years) believe that they have access to the right information on the environmental impact and energy consumption of digital technologies in their country. Further, slightly less than half of Europeans believe they have control over their own data, including how it is used online and with whom it is shared (48%, similarly to last years). Also, one third (33%) of Europeans continue to think that they cannot rely on the information they see online (35% in 2024). And only 42% of Europeans consider that their country is ensuring a safe digital environment and content for children and young people, a worrying number, despite the slight improvement over last year (39%). Overall, almost half of Europeans (48%) are worried about the safety of children online in their country (a slight improvement compared to last year (53%)).

EU-27 overview

The Commission, supported by the 2024 and 2025 studies, has identified **over 2 000 initiatives that implement digital rights and principles across the EU-27** by the end of 2024. Initiatives range from all sorts of legal instruments, policy measures, financial instruments, research, innovation and collaboration projects, communication campaigns, harmonisation and standardisation actions, educational tools, and monitoring initiatives.

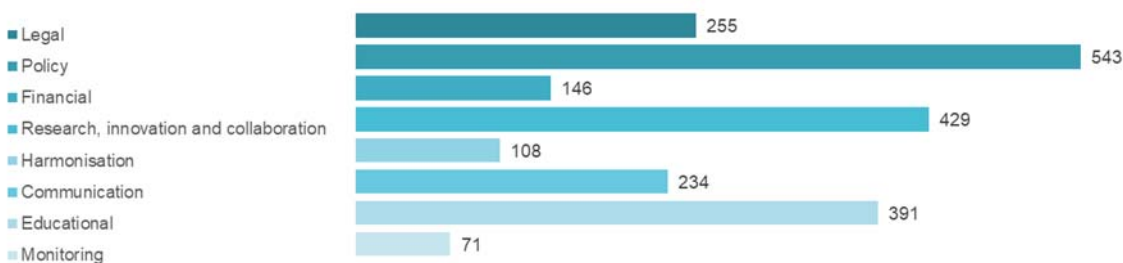| Type	Value
Legal	255
Policy	543
Financial	146
Research, innovation and collaboration	429
Harmonisation	108
Communication	234
Educational	391
Monitoring	71

Figure 1. Types of implementation initiatives found, per type of initiative

The total number of initiatives has been steadily growing over the years, with new initiatives peaking in 2023. While fewer digital rights initiatives were launched in 2024, the total number of ongoing initiatives is still increasing, with most initiatives running for several years.
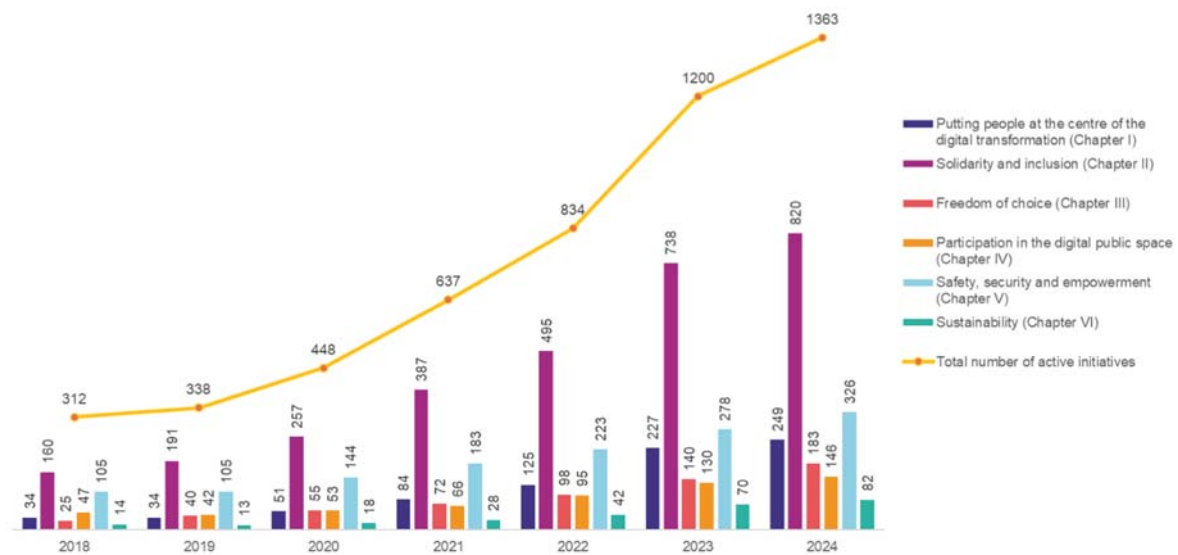

Figure 2. Number of ongoing implementation initiatives, per year and by Declaration Chapter
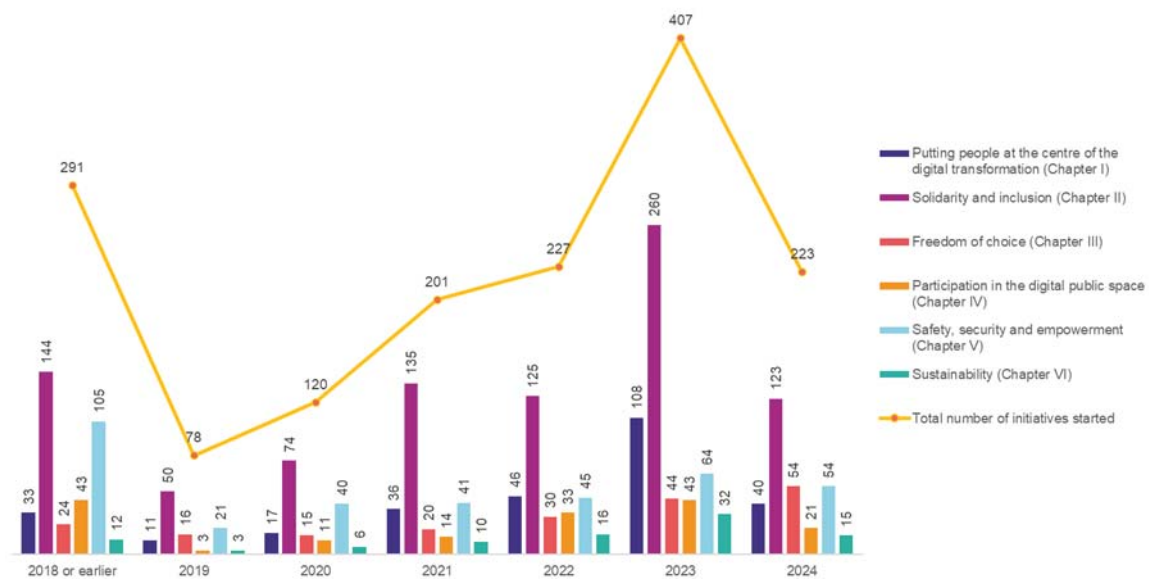

Figure 3. Number of launched initiatives per year and by Declaration Chapter

The analysis of digital rights initiatives shows that **most activity across the EU-27 is associated with two main Declaration areas: Solidarity and inclusion** (Chapter II) **and Safety, security and empowerment** (Chapter V). Member States are particularly active in the area of Digital education, training and skills (II), as well as A protected, safe and secure digital environment (III). However, the biggest gaps seem to persist in the area of Freedom of choice (Chapter III), Participation in the digital public space (Chapter IV) and in particular Sustainability (Chapter VI).
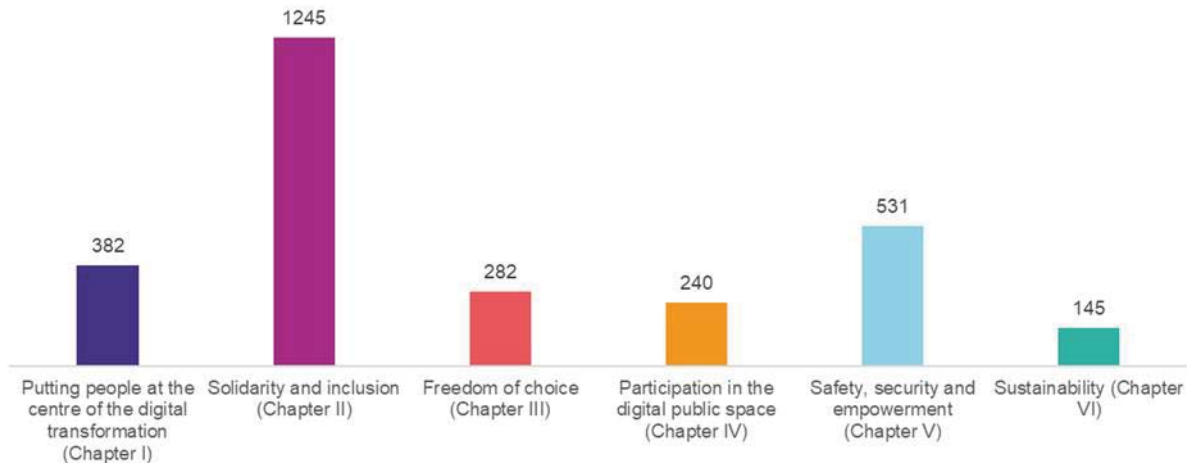

Figure 4. Number of implementation initiatives by Declaration Chapter

Most digital rights initiatives are led by government organisations (over 80%), such as ministries, public agencies and municipalities. A smaller number of initiatives are led by (National) Human Rights Institutions, civil society and industry stakeholders. Furthermore, the vast majority of digital rights initiatives are being developed **at national level** (close to 90%), while less activity is visible on the international, regional and local levels.

Overview of Member States activity

Initiatives that implement digital rights and principles were identified in all EU-27 Member States. In terms of overall activity, an average of 77 initiatives per country were identified. In addition to country-specific initiatives, 92 EU-wide initiatives stemming from EU legislation and policies were identified.

Seven Member States are the frontrunners in terms of their overall activity in implementing digital rights initiatives, with more than 100 initiatives each in place. This is the case of Portugal, Luxembourg, Spain, Malta, Italy, Austria and Belgium. On the other hand, the fewest digital rights initiatives were identified in four Member States which launched half of the average or fewer initiatives, namely Slovakia, Latvia, Slovenia and Estonia.
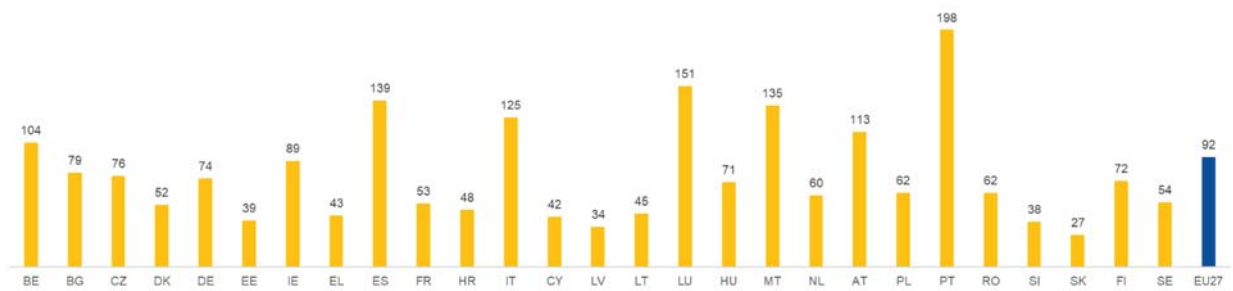
Figure 5. Number of implementation initiatives by EU-27 Member State

When it comes to **new activities launched in 2024, five Member States were particularly active**: Malta, Spain, Austria, Sweden and Luxembourg, with 15 or more new initiatives launched. It is worth noting that four of these Member States are also those that are most active overall. On the other hand, limited activity (with 5 or less new initiatives) was noted in 15 Member States. Although Greece, France, Lithuania and Slovakia have ongoing digital rights initiatives, no new initiatives were identified in 2024.

It is important to note that the number of initiatives does not fully reflect the extent to which a digital right or principle is protected and promoted. Some initiatives, such as political strategies at national level, may include a wide range of sub-actions or run over several years, while other initiatives might be very concrete or target a specific category of individuals, such as the elderly. All types of activities can be relevant at their corresponding scale. The overall number of digital rights initiatives however gives an important indication regarding the activity of Member States, their priorities and gaps.

Impact of digital rights initiatives across EU-27 Member States

Besides tracking the activity of Member States on digital rights and principles, it is also important to estimate the actual level of implementation of their initiatives on the ground and therefore to what extent the digital rights are effectively protected. When looking at the impact indicators framework[5], it appears that authorities which implement initiatives (notably governments, supported by industry and civil society) tend to have more optimistic views on the impact of digital rights initiatives compared to how they are perceived by citizens.

Overall, the indicators framework suggests that **the effective implementation of digital rights and principles remains limited, estimated to be applied only at 61%** on average and across all Declaration areas. This shows that significant gaps persist and the implementation of digital rights and principles require further attention from the Member States.

The **biggest impact and the most visible results (67%) are seen for horizontal commitments related to** *Putting people at the centre of the digital transformation* as per Declaration Chapter I. This shows that Member States overall recognise the importance of a human-centric digital transformation and implement measures on a rather strategic level, but that more operational action in more concrete Declaration areas is needed.

---

[5] Developed by the support study. Impact indicator framework explained in the Methodology part of this Annex.

The second-best implemented commitments appear to be those related to **Solidarity and inclusion** *(Chapter II),* standing at 64%. Member State focus on this area is not surprising, as several commitments in this chapter are closely related to Digital Decade targets measured by concrete indicators.

On the other hand, initiatives in the area of *Participation in the digital public space (Chapter IV)* and *Safety, security and empowerment (Chapter V)* seem to show only limited protection of digital rights and principles, regardless of Member States' efforts in the security and safety space linked to Chapter V.

While Figure 6 below does not show significant differences in the implementation of different Declaration chapters, the difference can be seen much more clearly in the specific country reports.

Figure 6. Impact of digital rights initiatives by chapter.

It is worth noting that some Declaration Commitments are rather broad, and progress has so far proven to be more difficult to measure, partly due to lack of available EU-27 data. This challenge is visible across the various Declaration chapters, but especially in the area of *Participation in the digital public space (Chapter IV)*. A more solid and complete monitoring framework would help to gain a full picture[6].

Overview of Member States' impact

The impact indicator framework shows that measures in **nine Member States show a very good level of implementation on the ground (75% and more).** This is the case of Luxembourg, Malta, Italy, Austria, Ireland, Finland, Sweden, Denmark and Poland. Among these Member States, good impact is estimated mainly in the area of *Solidarity and Inclusion* (four Member States) and *Putting people at the centre of the*

---

[6] See Recommendations of the Study to support the monitoring of the Declaration on Digital Rights and Principles, available here: https://digital-strategy.ec.europa.eu/en/news-redirect/883230

digital transformation (three Member States). On the other hand, the indicators show a **limited protection of digital rights and principles (less than 50%) in 14 Member States**. The biggest implementation gaps in those Member States exist in the area of *Safety, security and empowerment* (eight Member States) as well as *Participation in the digital public space* (six Member States).

A country-specific analysis of both implementation initiatives and their estimated impact is available in the individual Digital Decade country reports. The country reports include an overview of the overall activity of the Member State, the best and least implemented areas of the Declaration, the estimated impact of measures including country-specific Eurobarometer results, as well as country-specific recommendations.

The following chapters of this monitoring report assess the implementation of digital rights and principles divided into six main Chapters and thirteen action areas of the Declaration in which the EU and the Member States committed to act. The monitoring identifies measures taken across the EU, focusing on 2024 action across the Member States, and provides good practices. The monitoring report also presents the key 2025 Eurobarometer results and estimates the impact of these measures for each of the Declaration chapters.

Monitoring of Digital Rights and Principles

Chapter I - Putting people at the centre of the digital transformation

Putting people at the centre of the digital transformation of our societies and economies is at the core of the European Union vision outlined in the general objectives of the Digital Decade policy programme (Article 3) and the European Declaration on Digital Rights and Principles. The EU believes that digital technology should benefit everyone and empower them to pursue their aspirations, in full security and respecting their fundamental rights.

Overall, **people's awareness of digital rights has not increased in recent years**. According to the 2025 Special Eurobarometer survey[7], **59% of citizens are aware that the rights they have offline should also be respected online**. The share of the population aware of their digital rights was at 62% in 2024, and at 57% in 2023).

Most people seem to be well aware of their digital rights in the Netherlands and Slovenia (82%), followed by Finland, Lithuania and Luxembourg (81%). In 2024, the Netherlands, Luxembourg and Lithuania were also among the Member States with the greatest awareness of digital rights in the EU (85%, 81% and 79%, respectively). On the contrary, more than half of citizens are not aware of their digital rights in Bulgaria and Italy (58%, compared to 64% and 49% respectively in 2024), as well as in Romania (55%).

However, **people's perceptions of how their rights are protected in the digital environment remains rather negative**. Less than half of citizens (44%) indicated that they felt well protected in the digital space (similar to 45% in 2024). This could indicate a slightly negative trend since 2023 (50%), despite increasing efforts in this area. Furthermore, a large part of the population (41%) still does not feel well protected in the digital environment (44% in 2024, 36% in 2023). Citizens feel most protected in Malta (66%) and Ireland (61%), while more than half of people in Greece (57%, +6 percentage points) are worried.

Based on the impact indicator framework developed by the support study[8], taking into account both available data and perceptions of citizens, **67% of the commitments in this chapter are estimated to have been implemented** (2023 data). The indicators suggest that Member State action in this area has the most effective impact on the ground among all Declaration chapters. This has notably been the case in Luxembourg (82%), Ireland and Italy (both at 79%). It is worth noting that this estimation takes into account available EU27 data, in this case covering 3 out of 4 commitments in this chapter (not *1d)*.

EU action

In line with the Declaration, the European Union committed to **strengthening the democratic framework of digital transformation**, and to ensuring that the **values of the EU and the rights of individuals as recognised by EU law are respected online as well as offline** *(1a, 1b).* This human-centric vision of digital

---

transformation is at the core of relevant EU landmark legislation, such as the Digital Services Act (DSA) or the Artificial Intelligence (AI) Act, which are discussed in more detail in the next chapters of this report.

The EU and its Member States have also committed to ensuring **responsible and diligent action by all actors in the digital environmen**t. Besides digital regulation, a number of stakeholder initiatives have been taken, covering areas such as disinformation, artificial intelligence and sustainability, as will be explained elsewhere in this document *(1c).*

The EU has been particularly active in promoting this vision of digital transformation on the international scene, with the aim of inspiring its partners (*1d*). At **multilateral** level, the Declaration provided a strong basis for the ambitious United Nations **Global Digital Compact** **(GDC)**, the first comprehensive framework for global digital governance agreed at the Summit of the Future in September 2024. The GDC outlines a global vision and a set of commitments for the digital future at global level, reflecting EU priorities on how to reconcile human rights, democracy and the rule of law in this new area of digital governance. One of its key objectives is to foster 'an inclusive, open, safe and secure digital space that respects, protects and promotes human rights.' The UN Secretary-General presented a compact implementation map to reflect progress made on GDC implementation and follow-up at the United Nations Commission on Science and Technology for Development (CSTD) annual session in April 2025 in Geneva. The UN Office for Digital and Emerging Technologies, set up in January 2025, will support follow-up and implementation of the GDC. Other implementation steps include creating the International Scientific Panel on AI and the Global Dialogue on AI Governance.

The DSA incorporates universal principles such as giving agency over content moderation by online platforms back to citizens, and ensuring an undistorted information ecosystem. These universal principles are also reflected on the global stage, including in the UNESCO Guidelines on the governance of digital platforms.

The Commission is proactively promoting the EU digital transformation model at the Organisation for Economic Co-operation and Development (OECD), including through the Global Partnership on AI (GPAI).

The voluntary Code of Conduct for generative AI, agreed by G7 Leaders in 2023 and reflecting the key features of the EU's AI Act, was further endorsed by the OECD and strengthened through a new monitoring mechanism. The Commission continues to promote the 'Data Free Flow with Trust' initiative, reflecting the idea that data protection enables data flows, which increases trust in the digital economy. This is shaping the G7/20 discussions and supporting the work of the OECD. In the area of internet governance, the EU is committed to promoting its human-centric vision and interests in global multi-stakeholder institutions, including standardisation bodies. This encompasses concrete policies related to internet openness and security, as well as setting the global internet policy agenda.

In 2024, the Commission continued to promote its human-centric approach within its network of **bilateral** digital partnerships with 'like-minded' partners such as the USA, India, Japan, South Korea, Singapore and Canada. Cooperation was stepped up for cooperation on research collaboration, regulatory policy and standardisation. For instance, Digital Partnership Councils were held with Japan and the Republic of Korea in 2024, advancing cooperation on topics such as AI, connectivity, digital identities and trust services, data governance, online platforms and cybersecurity. The EU also discussed cooperation on AI and secure connectivity at the sixth EU-US Trade and Technology Council ministerial meeting in April 2024.

The EU also continued to discuss its approach to digital policy with key partners through Digital Dialogues, such as the one with Brazil, which took place in February 2025. The Digital Dialogue with Australia, relaunched in June 2024, notably discussed AI, data and cybersecurity, and agreed on increased and systematic cooperation on platforms.

In October 2024, the Commission also held a Regulatory Dialogue on digital policies with Western Balkans countries (Albania, Kosovo*[9], Montenegro, North Macedonia and Serbia) focused on AI, platforms, cybersecurity (including the 5G cybersecurity toolbox) and digital identity. It also approved their adopted Reform Agendas, which set out specific steps to align national legislation to EU digital rules by 2027, and allow payments under the Reform and Growth Facility upon completion of these steps.

A growing number of digital cooperation initiatives are supported by instruments such as the Neighbourhood, Development and International Cooperation Instrument – Global Europe (NDICI – Global Europe), the Connecting Europe Facility and Horizon Europe. In line with the 'Team Europe' approach, the Commission and Member States joined forces and set up a coordination platform aimed at strengthening the EU's global role in supporting a human-centric model of digital transformation: the Digital for Development (D4D) Hub. In 2024, the D4D Hub advanced digital partnerships, investments and actions in the areas of digital governance, connectivity and entrepreneurship, e-Services, gender and cybersecurity. These were implemented in four regions: Sub-Saharan Africa, Latin America and the Caribbean, Asia-Pacific, and EU neighbouring countries. It also strengthened policy dialogues, multi-stakeholder relations, the private sector and civil society engagement to boost a human-centric digital transformation in partner countries.

The EU also has a growing portfolio of free trade agreements[10] and digital trade agreements[11], which was expanded most recently with agreements with Japan, Singapore and the Republic of Korea. These 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.

Lastly, the Joint Communication on the International Digital Strategy, just published in June 2025, sets the ground for strengthening the EU role as a global digital player, advancing its strategic interests in the field of technology and digital transformation and supporting the digital transformation of partner countries.

Member State action

Overall, Member States had launched 382 initiatives related to implementing a human-centric digital transformation (*Chapter I*) by the end of 2024, according to the support study. The highest number of initiatives focus on strengthening the democratic framework for a digital transformation that benefits everyone *(1a).* This shows that, overall, Member States recognise the importance of a human-centric digital transformation and are implementing measures on a strategic level. Most initiatives are led by

---

*[9] This designation is without prejudice to positions on status, and in line with UNSCR 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.

[10] Free Trade Agreements with comprehensive digital trade chapters have been concluded with the United Kingdom, New Zealand and Chile, and are ongoing with India, Indonesia, Thailand, Philippines and Malaysia.

[11] Signature of the EU-Singapore Digital Trade Agreement took place on 7 May 2025. Negotiations for the Digital Trade Agreement with Korea were concluded in March 2025. Rules on cross-border data flows with Japan, complementing the EU-Japan Free Trade Agreement, entered into force in July 2024.

government organisations (83%), with fewer initiatives led by civil society, industry or National Human Rights Institutions. Initiatives are predominantly related to policy (31%) or research and technology projects (22%). The vast majority of initiatives are put forward at national level (86%), while only 3% have been carried out at regional and local level.

As regards **2024 action,** it is worth highlighting the first edition of International Digital Rights Days, on 10-11 December 2024, organised by the Cities Coalition for Digital Rights and coordinated by Bordeaux Métropole (**France**) and the City of Porto (**Portugal**). The event is planned to be repeated annually. With 50 international partners organising 20 events and campaigns in 2024, the Days aim to be an opportunity for cities to engage locally with residents on their digital rights, and to join forces with civil society organisations, public administration and policy makers that share the same commitment to raising awareness about digital rights and that promote responsible and diligent action *(1a-1d)*.

At local level in **the Netherlands**, the municipality of The Hague is working on a Digital Rights Agenda to ensure that the city uses the benefits of digitalisation in a responsible way *(1a-1c)*.

The federal government of **Germany** has put forward a Strategy for International Digital Policy. The strategy is based on key principles that guide Germany's international action, the first one being to 'protect fundamental and human rights – online and offline'. The government notably aims to 'take an active stance against government and non-government behaviour in the digital space that undermines fundamental rights, human rights or democratic basic orders'. Germany also aims to 'advocate for a global, open, free and secure internet', 'enhance value-based technology partnerships', 'promote human-centric and innovation-friendly rules' and 'strengthen a secure and sustainable global digital infrastructure'. *(1d)*

Best practice

The government of **Spain** has launched a Digital Rights Observatory to promote awareness, discussion and monitoring of digital rights among citizens and businesses, based on the Spanish *Digital Bill of Rights* (2021). The Observatory aims to provide an open, inclusive and participatory space, to inform citizens about progress, advantages and challenges in the field of digital rights and to promote good practices. The Observatory offers concrete projects for 2024-2026, including a plan on how to promote digital rights in Spain, in the EU and with Latin American partners; communication activities, events and courses to promote digital rights; the organisation of the first World Digital Rights Summit; and the creation of a monitoring platform for digital rights. More than 150 entities and 350 experts are involved in this project, including experts in the field of digital rights and technology, and representatives of public institutions and civil society organisations. The Observatory is mainly funded by the Recovery, Transformation and Resilience Plan through NextGenerationEU Funds, via Red.es, a public entity attached to the Ministry for Digital Transformation and Public Administration (up to 80%, with an overall budget of EUR 4.78 million). The project is co-financed by universities and other private actors.

Chapter II - Solidarity and inclusion

With the Declaration on Digital Rights and Principles and the general objectives of the Digital Decade, the European Union and its Member States stress the need to promote solidarity and inclusion with regard to

digital technology and services to support a fair and inclusive society and economy. They have notably committed to making sure that the design, development, deployment and use of technological solutions respect fundamental rights. They have also committed to a digital transformation that leaves nobody behind, which should benefit everyone, achieve gender balance, include in particular elderly people and people living in rural areas, ensure accessibility for persons with disabilities, and include marginalised or vulnerable people. In the context of inclusion, the EU and its Member States have also undertaken to develop a digital transformation that promotes cultural and linguistic diversity.

In the Declaration and as general objectives, the EU and its Member States have also undertaken to develop adequate frameworks so that all market actors benefiting from the digital transformation assume their social responsibilities and make a fair and proportionate contribution to the costs of public goods, services, and infrastructure, for the benefit of all people living in the EU.

Overall, 1 245 Member State initiatives related to implementing an inclusive digital transformation (Chapter II) were identified by the support study[12], making it **the most important area of Member State activity** by the end of 2024. The highest number of initiatives focus on the section Digital education, training and skills, especially with regard to promoting high-quality digital education and training, including with a view to bridging the digital gender divide *(4a)*.

The vast majority of initiatives are led by government organisations (88%), with only a small share of actions initiated by civil society, industry or National Human Rights Institutions. Initiatives are predominantly related to policy (25%), followed by educational measures (23%) and research and technology projects (22%). Most initiatives are put forward at national level (89%), supported by a relatively high number of city initiatives (45).

Based on the impact indicator framework developed by the support study, taking into account both available data and perceptions of citizens, **64% of the commitments in this chapter are estimated to have been implemented** (2023 data). The indicators suggest that Member State action in this area has the second most effective impact on the ground among all Declaration chapters. This has notably been the case in the Nordic countries, namely Denmark (78%), Finland (77%) and Sweden (75%), as well as in Malta (78%). It is worth noting that this estimation takes into account available EU27 data, in this case covering 12 out of 17 commitments in this chapter. The main gaps remain notably in the area of *Fair and just working conditions*, where 3 out of 5 commitments do not have any available data sources for the moment.

EU action

A number of EU digital regulatory instruments are contributing to the development and deployment of technological solutions that better respect fundamental rights *(2a).* The **AI Act**, which entered into force on 2 August 2024, addresses potential risks to citizens' health, safety, and fundamental rights. It provides developers and deployers with clear requirements and obligations regarding specific uses of AI, while reducing administrative and financial burdens for businesses to facilitate innovation. It bans the use of certain AI applications that are incompatible with European values, while imposing certain requirements on AI applications that are classified as 'high risk'. For deployers that provide public services and certain

---

[12] Study to support the monitoring of the Declaration on Digital Rights and Principles, available here: https://digital-strategy.ec.europa.eu/en/news-redirect/883230

private operators, a fundamental rights impact assessment is required. Finally, transparency obligations have been established so that citizens are informed when they interact with or are exposed to AI applications. Further to the adoption of the AI Act, preparing and adopting implementation measures has started (see below Chapter III Freedom of Choice)

Online platforms and search engines are crucial enablers for exercising fundamental rights worldwide, in particular freedom of expression and information. For this reason, the European Union has passed the **Digital Services Act (DSA)**, which lays down due diligence obligations for intermediary services to protect fundamental rights. The DSA empowers and protect citizens and ensures an undistorted information ecosystem in full respect of freedom of speech.

The DSA's transparency measures are crucial to allow society at large to scrutinise the moderation practices of online platforms and search engines. Users whose content or accounts have been restricted can: appeal against moderation decisions to the services' internal complaint handling systems; go to court; make use of one of the DSA's out-of-court dispute resolution bodies; or lodge a complaint with their national digital services coordinator.

At the core of democracies is trust and belief in an open society. The DSA facilitates this, by requiring platform providers to be fully transparent about their online moderation practices in the EU. Among other things, this includes an obligation to provide users with a statement of reasons when their content is removed or restricted, and information on how to appeal the decision; and an obligation to publish transparency reports, which include information about their content moderation practices, such as the number of take-down orders they have received from authorities in the EU and how many pieces of content they have removed.

Moreover, online platforms have to be clear in their terms and conditions about their content moderation policies and what types of legal content they allow or restrict on their services. Platforms must carefully enforce their rules while respecting the right of users to express themselves freely. They have to publish their content moderation decisions in the 'DSA Transparency Database'. This includes information on why they have removed content or restricted access to someone's account, and the number of users affected by these measures. Online platforms must also provide information about their algorithms and explain why users see certain content. For example, platforms must inform about the criteria used to rank and display content and the factors influencing content moderation. Additionally, providers of very large online platforms and search engines are obliged to conduct and publish risk assessment reports annually, as well as to undergo yearly external audits and to publish their audit and the audit implementation reports. The audits cover all obligations they have under the DSA.

The principle that **a digital transformation should leave no one behind** *(2b)* notably concerns people with disabilities. In 2024, the Commission continued to implement the Strategy for the Rights of Persons with Disabilities 2021-2030, including its chapter on accessibility. Regarding the latter, the Commission monitors and enforces the Member States' implementation of the European Accessibility Act Directive 2019/882, which had to be transposed by June 2022. In the meantime, at the request of the Commission (standardisation request (request M/587), standardisation bodies have been revising three existing standards and creating three new ones aimed at improving accessibility of IT equipment.

Efforts are also being undertaken through **AccessibleEU**, one of the flagships of the Strategy, to support the implementation of EU accessibility legislation, including by enhancing the capacity of digital professionals in the EU in matters related to accessibility for persons with disabilities. AccessibleEU is a resource centre on accessibility working on areas such as built environment, transport, information and communication technologies to improve accessibility in the EU in order to ensure that persons with disabilities participate in all areas of life on an equal basis with others. Since its start, it has organised 178 events, either at EU or national level, and attracted over 35 000 participants. AccessibleEU has created a Community of Practice on accessibility, which currently has over 3 400 members. The associated digital library holds over 300 good practices and 260 references on accessibility. So far, six guides (plus one item of support material) and one study have been published covering accessibility matters related to legislation, standards, cognitive accessibility, AI and many others.

Member State action

In 2024, many Member State initiatives were ongoing on inclusion, with many of them running over several years. For example, **Ireland** continued to implement its Digital Inclusion Roadmap for 2030 the objective of which is to make Ireland one of the most digitally inclusive countries in the EU and to give everyone the opportunity to use digital services, including digital public services, in a meaningful way.

In **Romania**, the EduClick project aims to reduce the digital divide in education by donating used computers to schools, NGOs, and institutions that work with disadvantaged communities. The project was running during 2023-2024 and was co-financed by the EU. In **Czechia**, the project IT's for girls! which ran throughout 2024 allowed women working in IT to visit primary and secondary schools to share their stories of how they got into IT, show that women are an important part of the IT world, present employment and study opportunities, and provide support to students in deciding which direction to take.

At the same time, in **France**, Bordeaux Metropole developed a new project in 2024, 'A look at digital suffering', collecting testimonies of citizens' difficulties in using digital technology, including how these affect their well-being. The results of this work will allow reflection to continue on the right place for digital technology, to guarantee digital inclusion for all.

Best practice

In **Slovakia**, the project Digitálni seniori aims to improve the digital skills of older and disadvantaged individuals. It offers both in-person and e-learning training sessions to help participants become more proficient in using digital technologies. Upon completing the training, participants receive tablets with data packages to continue practicing their new skills. Overall, almost 23 000 older people successfully finished the digital skills training. In October 2024, as part of the 'Month of the Elderly', a series of events took place across the country to educate older people about digital literacy, internet safety, media literacy and prevention against online fraud. The project is implemented by a Slovak Ministry under the Recovery and Resilience Plan.

Connectivity

The Declaration states that everyone should have access to affordable and high-speed digital connectivity everywhere in the EU. Under the general objectives of the Digital Decade policy programme, the EU and Member States must ensure that digital technologies and services 'are accessible to all, everywhere in the Union'. This is a key prerequisite for giving individuals equal chances in an increasingly digitalised world.

According to the 2025 Special Eurobarometer[13], **a majority of Europeans (57%) believe that they have access to an affordable high-speed internet connection** (57% in 2024, 53% in 2023). Nevertheless, one third (33%) stress the need for better connectivity, especially people in Greece (58%).

EU action

The Declaration aims to ensure that everyone has **access to high-quality connectivity, wherever in the EU, including those with low income** *(3a)*. The Gigabit Infrastructure Act (GIA) entered into force in May 2024, and most of its provisions will be applicable from November 2025. The GIA aims to ensure a faster, cheaper, and simpler roll out of Gigabit networks, addressing the main hurdles such as expensive and complex procedures for network deployment. The Act is instrumental to achieving the 2030 Digital Decade target on connectivity: ensuring cross-EU access to fast Gigabit connectivity and fast mobile data by 2030. As provided in the GIA, the Body of European Regulators for Electronic Communication (BEREC), in close cooperation with the Commission, is preparing guidelines on the coordination of civil works and on access to in-building physical infrastructure; both sets of guidelines are due by November 2025.

Moreover, in order to ensure reliable, high-capacity digital infrastructure, the Commission, as provided in its 2025 Work Programme, intends to propose a **Digital Networks Act**, which will incentivise cross-border network operation and service provision, enhance industry competitiveness and improve spectrum coordination.

To protect and promote a **neutral and open Internet** *(3b)*, the Commission closely monitors the implementation of the provisions of Regulation (EU) 2015/2120 on open internet access in the Member States, including through the participation in BEREC and its Open Internet Working Group, alongside the Member States' national regulatory authorities.

Member State action

To ensure access to **high-quality and affordable connectivity for all** *(3a)*, Member States continue to invest in increasing their high-speed internet and 5G coverage, often with support from the Recovery and Resilience Facility (RRF). These investments usually span several years. For instance, **Croatia**'s broadband investment of EUR 133 million, supported under the RRF, aims at increasing the availability of electronic communications networks in areas where there is no commercial interest, by providing gigabit connectivity to households and companies, in line with the objectives of the European Gigabit Society. These investments will be made in fixed networks (VHCN) in Croatia, in rural and urban areas. They should cover at least 100 000 additional households in white NGA areas with broadband access of at least 100 Mbit/s for downloading (upgradable to 1 Giga) by June 2026.

---

[13] 2025 Special Eurobarometer Report on the Digital Decade, available here: https://digital-strategy.ec.europa.eu/en/news-redirect/883227

Member States produce annual monitoring reports on **neutral and open Internet** (*3b*). As of 2024, it has been reported that 21 national regulatory authorities provided an internet access service quality monitoring tool, and 10 Member States had put in place certified monitoring mechanisms under Article 4(1)(d) of the Open Internet Regulation, enabling consumers to take action against broadband providers which fail to deliver on the speeds committed to in contracts. Concerning traffic management measures, most reports indicate that blocking is only performed for reasons of network security and integrity.

Best practice

In March 2024, **Belgium** introduced a new telecom social tariff called the Social internet offer. This discounted rate for fixed internet is offered to individuals and families in a vulnerable situation (social aid beneficiaries) and financed by the telecom sector. The rules define the maximum price and the minimum technical requirements that telecom operators must meet for contracts benefiting from the discount; a 50% reduction of installation fees also applies. These rules are mandatory for VOO, Proximus and Telenet, and voluntary for other telecom operators. With over 20 000 contracts signed already, the offer aims to target a much wider audience.

Digital education, training and skills

The Declaration states that everyone has the right to education, training and lifelong learning and should be able to acquire all basic and advanced digital skills. The general objective of the Digital Decade policy programme commits to 'bridging the digital divide, achieving gender and geographic balance by promoting continuous opportunities for all individuals, developing basic and advanced digital skills and competencies' .

According to the 2025 Eurobarometer[14], **the majority of Europeans (60%) feel that they are getting necessary basic or advanced digital education, training and skills**, with the best results in Malta (79%) and Luxembourg (75%). Almost one third of Europeans (29%) do not feel appropriately equipped for the digital decade, and this is especially the case in Greece (47%).

EU action

The EU committed to promoting **high-quality digital education and training, including with a view to bridging the digital gender divide** (*4a*) and to supporting efforts which allow all **learners and teachers to acquire and share the necessary digital skills and competences, including media literacy, and critical thinking** (*4b*). The EU also undertook to promote and support **efforts to equip all education and training institutions with digital connectivity, infrastructure and tools** *(4c)* and to give everyone the possibility to adjust to changes brought by the digitalisation of work through **up-skilling and re-skilling** *(4d)*.

The Commission recently launched a number of initiatives to strengthen basic and advanced digital skills and support bridging the digital gender divide (*4a*). In its March 2025 Communication '**The Union of Skills'**, the Commission outlined a strategy to improve high quality education, training, and lifelong learning. The strategy includes a number of flagship initiatives to support the development of resilient and adaptable

---

[14] 2025 Special Eurobarometer Report on the Digital Decade, available here: https://digital-strategy.ec.europa.eu/en/news-redirect/883227

education, training and skills systems and strengthen the provision of basic digital skills. The **Action Plan on Basic Skills** reaffirms the EU's commitment and ambition to support quality education for all. It promotes digital literacy as part of the basic skills set necessary for learning, working, and participating in society, as well as for handling cyberthreats and safely navigating technologies such as AI. The Commission will notably pilot a Basic Skills support scheme, so that every young person has strong reading, maths, science and digital skills.

As part of the Union of Skills strategy, the **STEM Education Strategic Plan** aims to reinforce digital skills, guided by its objectives to: anchor STEM as a strategic pillar in the EU's education and skills policy; build a stronger and more inclusive EU STEM talent pipeline; and advance women in STEM and inspire future innovators (*4b*). The STEM Education Strategic Plan aims to attract more women and girls to STEM studies, including digital studies and careers. The Commission plans to establish four new **digital skills academies** in AI, Quantum, Virtual Worlds and Semiconductors. The Commission will also launch the Industry-Academia network of the **Cybersecurity Skills Academy** in June 2025 and promote cyber-campuses for cybersecurity skills in various Member States.

In 2024, the Commission launched the mid-term review of the **Digital Education Action Plan**; based on the results of the review, the 2030 Roadmap on the future of digital education and skills to promote equal access to digital education for all will be issued later in 2025. A robust EU digital education ecosystem must prepare for the future and establish long-term partnerships with EU-based EdTech (education technology) and independently developed European solutions. An initiative on AI in education and training will lay down an AI literacy framework and support the integration of AI in education and training provision, addressing the need for online safety and digital well-being, tackling disinformation and misinformation, while promoting innovation in education.

In 2023, Member States reinforced their commitment to the objectives of the Digital Education Action Plan through the adoption of two **Council Recommendations on digital education and skills**[15]. Following on the adoption of the Council Recommendations, the Commission established two expert groups to create two sets of **guidelines aimed at the education and training community**: *Guidelines for accessible, well-designed and high-quality digital education content*, and *Guidelines for high-quality education in informatics*. In parallel, the Commission launched in January 2025 the process of updating its *Guidelines for teachers and educators on tackling disinformation and promoting digital literacy,* as well as its *Guidelines on the Ethical use of AI and Data in teaching and learning for educators (4c)*. These will be updated to reflect developments in the three years since their adoption with the objective of ensuring timely and relevant support for teachers and educators across the EU. Notably, the *Guidelines on tackling disinformation* will address the impact of generative AI on the creation of deceitful content (e.g. deepfakes), novelties in social media, influencers, and pre-bunking and will offer further guidance for policymakers. The *Ethical Guidelines on AI* will also tackle the impact of generative AI for education practices, provide an update on regulatory matters (in relation to the AI Act) and more hands-on activities for teachers. The guidelines are expected to be published in autumn 2025.

To help EU Member States overcome challenges in meeting both basic and advanced digital skills, the **Digital Skills Cluster** was launched under the Digital Decade policy in July 2024 under the leadership of

---

[15] Council Recommendation on the key enabling factors for successful digital education and training and Council Recommendation on improving the provision of digital skills and competences in education and training.

Slovenia. Its primary goal is to collect and share high-level initiatives at government level that can be replicated in Member States to boost digital skills. Furthermore, the Joint Research Centre (JRC) is working on a comprehensive **update of the Digital Competence Framework for Citizens** (DigComp) by the end of 2025 to take into account emerging technologies such as AI. In February 2025, the Commission published a [report](#) that analysed the Digital Skills Indicator to present the areas of digital skills, and the groups of adults that would require further digital skills development. In March 2024, the Commission published a [policy brief,](#) which underscores that digital under-skills are not the same as low digital skills**:** many under-skilled workers in fact possess high digital skills in general, but their skills are below those required for their job.

The **AI Continent Action plan** sets out actions to upskill and reskill workers to ensure a human-centric digital transition and raise awareness of AI among the wider EU society (*4d*).

To promote the development of advanced digital skills and increase the number of ICT specialists in Europe, the Commission is providing support to Member States to increase their offer of **joint academic programmes** and **short-term trainings** in key digital areas. The Commission, under the Digital Europe Programme, funds the design and delivery of higher education programmes and self-standing modules in advanced digital skills for developers and users of advanced digital technologies (e.g. AI, data analytics, virtual worlds, photonics, quantum, cloud and edge computing, and others). The stakeholders that are developing these state-of-the-art education and training programmes have increased to more than 435 organisations from 26 Member States. Furthermore, the Commission is working on establishing **digital skills academies**, with three new academies on AI, Quantum and Virtual Worlds planned for 2025.

Member State action

In the area of digital skills and education, in 2024 **Portugal** announced the launch of the first [National programme for Girls in STEM](#), to be launched in 2025. The programme proposes three axes of action: (1) education (from preschool to 12th grade), (2) higher education and (3) labour market. In the educational context, the initiative aims to stimulate the interest of young girls to pursue higher education courses and careers in these fields. To this end, a network of ambassadors and female 'role models' will be established. In teaching and work environments, the initiative aims to promote more inclusive and favourable conditions for the retention of women in the digital area. *(4a)*

Another measure announced by Portugal is the creation of the [Digital Skills Curriculum](#), which will allow every citizen to have a reliable tool to validate and prove their digital skills. A national platform for the certification and management of micro-credentials in digital skills will be integrated into the single public services portal, gov.pt. This platform will be updated based on the needs of the job market and the specific demand for digital skills. The Digital Skills Curriculum will also serve as a guidance tool, presenting training and development paths adjusted to the preferences of users and a changing job market *(4d).*

In **Poland**, the Ministry of National Education launched in 2024 a plan for the [Digital Transformation of Education Policy](#), with milestones to be achieved by 2027, 2030, and 2035. The plan sets the ground for changes in the education system and the implementation of investments in new technologies and defines the directions for the digitisation of education system in the short and long term. The aim is to promote high-quality digital education, with a specific focus on: the use of new technologies both by students and

teachers; developing students' critical thinking skills; equipping schools with appropriate digital infrastructure; and providing tools and training for teachers. *(4a, 4b, 4c).*

In **Lithuania**, an EdTech project running between 2022 and 2024, with a budget of EUR 30 million, was aimed at promoting the use of educational technologies, providing training for teachers, and developing digital content (*4c*).

> **Best practice**
>
> In **Ireland,** the Research Ireland Discover programme received approximately EUR 5 million in funding in 2024 to support 38 projects promoting diversity and inclusion in STEM. These initiatives are targeted at students in primary, secondary and third-level education and aim to deepen their understanding of what studying and pursuing a career in STEM entails. One of the projects, for instance, aims to address gender bias in computer science and cybersecurity, blending STEM with the arts and humanities by using immersive technology and storytelling methods. The funding was provided by the Department of Further and Higher Education Research, Innovation and Science and the Department of Education.

Fair and just working conditions

Everyone has the right to fair, just, healthy and safe working conditions and appropriate protection in the digital environment. The Declaration provides that people should be able to disconnect after working hours and benefit from a work-life balance.

The 2025 Special Eurobarometer[16] shows that **a stable majority (54%) of Europeans think that people working in the digital environment are benefitting from fair and healthy working conditions, and that they enjoy work-life balance** (55% in 2024). This is notably the case in Malta (72%) and Luxembourg (70%). On the other hand, one third (31%) hold the opposite view (32% in 2024), with most negative views coming from Greece (50%).

EU action

In April 2024, the Commission launched a formal two-stage consultation of the social partners on a potential EU initiative on the right to disconnect and telework, in line with Article 154 TFEU. The first stage of this consultation was carried out between April and June 2024 *(6a).* In addition, the Commission is currently working on gathering evidence on the impact of an 'always-on' work culture and possible implications of EU action in this area.

The review of the Display Screen Equipment Directive 90/270/EEC, which lays down minimum safety and health requirements for work with display screen equipment, is ongoing *(6b)*. In November 2024, the Advisory Committee on Safety and Health at Work adopted its Opinion on the review of Directive 90/270/EEC.

On 23 October 2024, the EU adopted **Directive 2024/2831 on improving working conditions in platform work** *(6c).* Platform work is a form of work in which organisations or individuals use an online platform to access other organisations or individuals to provide specific services in exchange for payment. The biggest

---

[16] 2025 Special Eurobarometer Report on the Digital Decade, available here: https://digital-strategy.ec.europa.eu/en/news-redirect/883227

revenues in this growing sector are estimated to be in the sectors of delivery and taxi services. The new rules address cases of misclassification of platform workers and ease the way for such workers to be reclassified as employees, guaranteeing easier access to their rights as employees under EU law. Moreover, workers will have to be **informed** about the use of automated monitoring and decision-making systems; and certain data may not be processed on digital labour platforms. In all cases, under the new rules, these systems must be monitored by qualified staff, who enjoy special protection from adverse treatment. Human oversight is also guaranteed for significant decisions such as the suspension of accounts. Member States have to transpose this directive into national law by December 2026.

According to the recent **Eurobarometer survey** on 'Artificial Intelligence and the future of work', most people in Europe believe that digital technologies, including AI, have a positive impact on their jobs, the economy, society, and their quality of life. 62% of respondents have a positive view of the use of robots and AI at work, and 70% believe these technologies improve productivity. At the same time, a large majority of respondents **support clear rules on the use of digital technologies**, for instance protecting workers' privacy (82%) and involving workers and their representatives in the design and adoption of new technologies (77%).

The Commission announced in its Work Programme 2025 that it would intensify implementation of the European Pillar of Social Rights, whose principles have guided efforts to tackle shared challenges in employment, skills and social issues since 2017. These principles were turned into tangible action through a dedicated Action Plan with headline 2030 targets. In 2025 the Commission will intensify implementation through a new action plan to be published later in 2025. The new Action Plan on the Implementation of the European Pillar of Social Rights will include initiatives looking at how digitalisation is impacting work. In her Mission Letter, Roxana Mînzatu, Executive Vice-President for Social Rights and Skills, Quality Jobs and Preparedness, has been mandated to focus on the impact of digitalisation on the world of work, including with an initiative on algorithmic management and possible legislation on AI in the workplace, following consultation with social partners *(6d)*.

The Commission continues exploring the context, challenges, opportunities, and trends in algorithmic management at the workplace.

Member State action

In 2024, 25 EU Member States, together with the European Commission, the European Parliament, European Economic and Social Committee, the majority of European social partners and civil society signed the La Hulpe Declaration, renewing their commitment to the European Social Model to continue making social and economic progress, combining increased competitiveness and productivity with equal opportunities, promoting more quality jobs and fair working conditions.

This Declaration notably addresses the online environment and its impact on working conditions. Member States notably agreed that further evaluation and additional actions may be required to ensure fair working conditions in key areas for the digital age such as telework, the right to disconnect, incorporating the 'human in control' principle for AI in the world of work, regulating algorithmic management, and information and consultation of workers.

Member States are currently implementing amendments to national legislation following the adoption of the Platform Work Directive and many Member States have ongoing communication campaigns about safety and health at work.

Several Member States have introduced specific legislation on telework, regulating aspects related to accessing telework, providing information to teleworkers, monitoring, compensation of costs and other.

> **Best practice**
>
> The right to disconnect in **Bulgaria** was introduced in March 2024 by an amendment of the Labour Code. It grants employees the right to disconnect, meaning they are not obliged to respond to employer-initiated communications such as email or, calls outside their working hours. Exceptions can be agreed upon in the individual employment contract or collective bargaining agreement. A right to disconnect has been adopted in national legislation in half of the EU Member States, including Belgium, Bulgaria, Croatia, Cyprus, Greece, France, Ireland, Italy, Luxembourg, Portugal, Slovakia, Slovenia, and Spain.

Digital public services online

The Declaration states that everyone should have online access to key public services in the EU. Specifically, the EU and Member States have committed to facilitating and supporting seamless, secure and interoperable access across the EU to digital public services designed to meet people's needs in an effective manner. These include in particular digital health and care services, such as access to electronic health records. A similar commitment is made in the general objective of the Digital Decade. In the Declaration, the EU and Member States committed to ensuring that people living in the EU are offered the possibility to use an accessible, voluntary, secure and trusted digital identity that gives access to a broad range of online services. The EU also aims to ensure that digital public services are accessible to citizens of any Member State without discrimination.

The 2025 Eurobarometer survey[17] shows that **the majority of Europeans (58%, as in 2024) find it easy to access digital public services**. This is notably the view of people in Malta (76%) and Luxembourg (75%). However, for almost one third (30%) of Europeans accessing such services remains a challenge, especially in Greece (45%).

EU action

In April 2024, the European Parliament and the Council of the EU adopted a **Regulation establishing the European Digital Identity Framework**, revising the current eIDAS Regulation (*7a*). With the new Regulation, all EU citizens will be offered the possibility to have an EU Digital Identity Wallet to access public and private online services all over Europe, with their security and personal data fully protected. Member States will have to provide **EU Digital Identity Wallets** (eID Wallets) to their citizens 24 months after adoption of implementing acts setting out the technical specifications for the EU Digital Identity

---

[17] 2025 Special Eurobarometer Report on the Digital Decade, available here: https://digital-strategy.ec.europa.eu/en/news-redirect/883227

Wallet and the technical specifications for certification. So far, nine **implementing acts** have been adopted, in November 2024 and April 2025, setting uniform technical standards and putting in place a robust certification framework. The Acts have been informed by requirements and specifications developed for the EU Digital Identity Toolbox and ensure uniform implementation of wallets across Europe.

In 2024, Romania and Finland joined other EU Member States in notifying their electronic identification (eID) schemes, bringing the total share of EU citizens now having access to electronic identification to 95%. The number of Member States with notified eID schemes has increased significantly, from just one in 2017 to 24 by 2025. This expansion represents a major advancement towards a more integrated and secure digital public service across Europe.

Under the Digital Europe Programme, Member States are participating in large-scale pilot projects aimed at testing wallets in everyday scenarios that benefit citizens, businesses, and governments. Since April 2023, these projects have involved **over 350 private and public entities from almost all EU Member States,** as well as **Norway, Iceland, and Ukraine**, exploring 11 different use cases.

- Nordic-Baltic eID (NOBID), involving Nordic and Baltic countries along with Italy and Germany, is currently piloting the use of EUDI wallets for SEPA instant payments.

- Potential involves over 140 public and private partners from 17 Member States and Ukraine. It aims to pilot six use-cases: access to online public services, mobile driving licenses, opening of bank accounts, SIM card registration, eSignatures and ePrescriptions.

- EU Digital Identity Wallet Consortium (EWC), led by Sweden, focuses on testing three use cases: digital travel credentials, payments, and organisation identity. This large-scale project (LSP) involves more than 50 public and private partners.

- Digital Credentials for Europe (DC4EU), led by Spain, is piloting the use of educational and professional qualifications and social security credentials, including the European Health Insurance Card and Portable Document A1 for seconded workers.

To support the piloting of EUDI Wallets, the Commission launched a second funding round for **pilot projects in 2024**, which saw strong interest from public and private actors across Member States. This initiative will support two pilot projects with a total investment of over EUR 23 million from the Commission. These projects, involving over 300 public and private entities from the majority of Member States, as well as Bosnia and Herzegovina, Moldova, Norway and Ukraine, are scheduled to start in Q3 2025 and will run for two years.

The Data Governance Act, applicable since 23 September 2023, complements the existing policy to make as much public sector information as possible available as 'open data', i.e. re-usable with as few restrictions and conditions as possible (*7b*). It provides mechanisms to make data available for re-use under controlled conditions or on grounds of commercial confidentiality. The Commission is currently working with Member States to ensure that the mechanisms needed to put this into practice are in place in all countries. Currently, eight Member States have not yet designated the necessary enforcement bodies. At the same time, funding is provided under Recovery and Resilience Fund actions to increase the public sector's capacity to implement the provisions on re-use of public sector information.

The Interoperable Europe Act, which entered into force in April 2024, set up a new cooperation framework for EU public administrations to ensure the seamless delivery of **public services** across borders, and to offer support measures promoting innovation and enhancing skills and knowledge exchange. It will help the EU and Member States to deliver better public services, interoperable by default, to individuals and businesses (*7c*). The Commission has started preparatory work on the new monitoring mechanism in collaboration with the Joint Research Centre and the expert group on interoperability of public services.

On this issue of health, the European Health Data Space (EHDS) Regulation, which entered into force on 25 March 2025 is a significant step forward in providing the public with additional rights to access, control, and share specific categories of their personal electronic health data using online services (*7c*). Empowering patients to securely access their own electronic health records (EHR) – both nationally and across borders – will contribute to more efficient healthcare delivery and improve the quality and quantity of health data for secondary use for research, innovation and health policy-making purposes. The Regulation will also create harmonised requirements on EHR systems regarding interoperability and logging capabilities. The main parts of the Regulation will apply from March 2029.

The EHDS will also help Member States reach the target set out in the Digital Decade Policy Programme, according to which 100% of EU citizens will have access to their electronic health records by 2030.

A number of specific actions will also contribute to the target: the e-Health Digital Service Infrastructure, which facilitates cross-border exchange of health data including patient summaries and e-prescription (with EU support and co-financing from EU4Health and CEF; multiple actions to support the development and uptake of the European Electronic Health Record Exchange Format (EEHRxF) in EHR products and services (with Horizon Europe, DIGITAL Europe and EU4Health funding); large health data infrastructures (with DEP funding); Genomics Data Infrastructure, European Cancer Imaging Platform, Intensive Care Unit data platforms – all under development; and the start of development in 2025 of a platform for the advanced integration of Virtual Human Twins.

Member State action

Many Member States continue to provide digital identity solutions to make interactions between citizens and public institutions easier. For example, in 2024, a new law in **Portugal** established that digital documents presented through the ID.gov application have equal legal value to original documents, requiring no additional validation. In **Luxembourg**, the MyGuichet.lu platform has offered a Virtual Meeting Room since 2024 that gives citizens a secure and confidential environment in which to connect to appointments by video conference with public administrations online. *(7a)*

With regards to the reuse of protected public sector data (7*b*), 19 out of 27 Member States have put mechanisms in place under the Data Governance Act. A consortium of statistical institutes from the Netherlands, Germany and Estonia is building capacity, partially financed by the Recovery and Resilience Facility.

On **e-health** *(7c),* all Member States now have some form of electronic health access service in place, be it regional or national, and have improved the extent of accessible health data categories, access technology and means, and the access opportunities for certain categories of people (scoring 82.7/100, DESI data from 2024, up from 79.1/100 reported in 2023).

In 2024, **Ireland** published the Health Information Bill, which provides a legal basis for the development and deployment of electronic health records in Ireland, along with legal provisions on the sharing of patient data for care and treatment. This will support fulfilment of Ireland's obligations under the European Health Data Space (EHDS) Regulation. Ireland also released ePharmacy, a national system that supports digital medical prescriptions, dispensing medication, and access to prescription and dispensing information for all, via a patient app and or patient portal. Healthcare professionals are also able to access this same information where required for direct patient care.

> **Best practice**
>
> **Czechia**'s eDoklady is a digital platform that allows citizens to store and manage their identification documents electronically with a digital ID card. The platform includes a mobile application that securely stores digital versions of ID cards, making it easier for citizens to provide identification without carrying physical documents. The initiative aims to streamline administrative processes and increase security by reducing the risk of document forgery. In 2024 and early 2025, Czechia extended the use of this platform to all main public administration authorities at national and local level, banks, the police, schools and universities, health insurance companies, post offices and polling stations.

Chapter III - Freedom of choice

The Declaration states that artificial intelligence (AI) systems should benefit people, including allowing them to make their own informed choices in the digital environment while being protected against risks and harm to health, safety and fundamental rights.

According to the 2025 Eurobarometer[18], **only a slight majority (53%) of Europeans believes that they are getting effective freedom of choice online** (52% in 2024 and 49% in 2023), **including when interacting with AI** (e.g., chatbots, digital assistants), with the highest score in Malta (74%). Almost one third (30%) of Europeans said they were sceptical (32% in 2024), especially the Greek public (42%).

Overall, 282 Member State initiatives implementing a free and fair digital environment (*chapter III*) had been by the end of 2024 identified by the support study[19]. This reveals the rather **limited activity of Member States in this area** in the past, which can be explained in part by the early phase of full enforcement of EU legislation, such as the AI Act, DSA and DMA. That said, **the number of newly launched initiatives is on the rise** with 54 new initiatives, most of which started in 2024.

The highest number of initiatives focus on the *section Interactions with algorithms and artificial intelligence systems*, and specifically on promoting human-centric, trustworthy and ethical artificial intelligence systems throughout their development, deployment and use, in line with EU values (*9a*) and ensuring an adequate level of transparency about the use of algorithms and AI, so that people are empowered to use them and are informed when interacting with them (*9b*).

---

[18] 2025 Special Eurobarometer Report on the Digital Decade, available here: https://digital-strategy.ec.europa.eu/en/news-redirect/883227

[19] Study to support the monitoring of the Declaration on Digital Rights and Principles, available here: https://digital-strategy.ec.europa.eu/en/news-redirect/883230

The vast majority of initiatives is led by government organisations (86%), with only a small share of actions initiated by civil society, industry or national human rights institutions. The initiatives are predominantly policy related (32%) or implementing research and technology solutions (27%). Though most initiatives are at the national level (81%), action in this area is also supported by relatively high numbers of city-level initiative (12%).

Based on the impact indicator framework developed by the support study, taking into account both available data and public perceptions, **the commitments in this chapter are estimated to be implemented at 63%** (2023 data). The indicators suggest that some Member States were quite effective in implementing these commitments on the ground, notably in Poland (78%). On the other hand, impact indicators show only limited impact of measures in this area in countries such as Cyprus and Sweden (44%), Luxembourg (43%) and Romania (31%). It is worth noting that this estimate takes into account the available EU27 data, which in this case covers 5 out of 8 of the commitments in this chapter.

Interactions with algorithms and artificial intelligence systems

The Declaration provides that AI systems should benefit people, including by allowing them to make their own informed choices in the digital environment while being protected against risks and harm to health, safety and fundamental rights.

EU action

The **Artificial Intelligence Act** (AI Act) aims explicitly to promote the uptake of human-centric and trustworthy AI while ensuring a high level of protection of health, safety, fundamental rights, in line with the Declaration (*9a, 9e*).

The AI Act entered into force on 2 August 2024. Provisions introducing obligations for AI developers and deployers are gradually becoming applicable. The bans on AI systems that are incompatible with fundamental rights became applicable on 2 February 2025. In order to facilitate the understanding of these provisions, the European Commission adopted Guidelines regarding prohibited practices, and Guidelines regarding the definition of an AI system on 4 and 6 February 2025 respectively. The Guidelines on prohibited AI systems specifically address practices such as harmful manipulation, social scoring, and real-time remote biometric identification. The listed practices are prohibited because they contradict the EU values of respect for human dignity, freedom, equality, democracy, and the rule of law as well as fundamental rights enshrined in the Charter of Fundamental Right of the European Union[20].

The provisions for general purpose AI will enter into force on 2 August 2025. To ensure effective implementation, on 30 September 2024, the Commission launched the process of drafting a Code of Practice, which is developed by the stakeholders themselves under the supervision of the AI Office. The Code of Practice is scheduled to be adopted before the related provisions become applicable.

---

[20] These include the right to non-discrimination (Article 21 Charter) and equality (Article 20), data protection (Article 8 Charter) and private and family life (Article 7 Charter), and the rights of the child (Article 24 Charter). The prohibitions in Article 5 AI Act also aim to uphold the right to freedom of expression and information (Article 11 Charter), freedom of assembly and of association (Article 12 Charter), freedom of thought, conscience and religion (Article 10 Charter), the right to an effective remedy and fair trial (Article 47 Charter), and the presumption of innocence and the right of defence (Article 48 Charter).

In the context of the Commission's **AI Continent Action Plan** launched on 9 April 2025, the Commission decided to set up a dedicated **AI Act Service Desk**. This is an information hub with simple, straightforward information on the application of the AI Act and the possibility to receive targeted answers to questions. It will include the Commission's Single Information Platform, as provided for in the AI Act. The platform will provide online interactive tools to help stakeholders determine whether they are subject to legal obligations and understand the steps they need to take to comply with the rules.

In parallel, the AI Board began its work, with its first meeting in September 2024. The AI Board is where national authorities meet to coordinate implementation in each Member State. The AI Board has two official support groups, the Scientific Panel and the Advisory Forum.

Furthermore, with the gradual implementation of the AI Act, the Commission launched the **AI Pact**, an initiative to accompany organisations in their compliance journey and foster early action by front-running organisations to foster the development and deployment of trustworthy AI. The **AI Pact** has been built on two main axes. On the one hand, it establishes a network of more than 2 300 stakeholders (including, but not limited to, companies, not-for-profit organisations, academics, public organisations, etc) who should contribute to the creation of a collaborative community, sharing their experiences and knowledge. In that context, the AI Office organises webinars for a better understanding of the AI Act and on how to prepare for its implementation and gathers insights into best practices and challenges faced by the participants. On the other hand, more than 190 companies providing or deploying AI systems (including multinational corporations and European SMEs, from diverse sectors (e.g. IT, telecoms, healthcare, banking, automotive, and aeronautics)) have accepted to sign pledges to take measures to anticipate compliance with key AI Act requirements as much as possible and to share corresponding good practices.

Member State action

Besides action at EU level with the AI Act, Member States are currently setting up and/or designating their national authorities, due by August 2025. On the one hand, the notifying authorities will oversee the assessment of AI applications before they are put on the market. And on the other hand, the market surveillance authorities will oversee the AI applications once they are on the market.

To support the implementation of the AI Act at national level and foster further use of a trustworthy AI, Member States have taken a wide range of measures in 2024. In **Sweden**, the Swedish Agency for Digital Government (Digg) and the Swedish Authority for Privacy Protection (IMY) created joint guidelines for the use of generative AI in the public sector, published in January 2025. The guidelines aim to increase the use of generative AI in public administration, including at regional and local level, promote the possibilities of using generative AI to support the business and ensure that the use complies with EU law. The guidelines will be continuously updated in order to be future-proof.

Meanwhile, **Latvia** signed a Memorandum of cooperation in December 2024 with Microsoft. In it, Latvia commits to continue working on the development of the National Centre for Artificial Intelligence and other digital initiatives in cooperation with Microsoft. The Memorandum aims to promote the use of AI and digital solutions for modernising public administration processes, as well as to develop the innovation and technology ecosystem in the country.

Poland has launched the AI Task Force, which offers a wide range of support and expertise in the development and implementation of AI projects, tailored to their specific needs and sector characteristics.

The task force provides technological, ethical and legal advice and training. It supports AI projects from the conceptual phase, through design to effective implementation.

Bulgaria put forward the Action Plan of the Open Government Partnership Initiative. This aims to implement various forms of effective public dialogue to develop common standards on the use of AI in the digitisation process to ensure guarantees of equal access and respect for human rights. A new working group under the Minister of Electronic Governance should develop these common standards.

France hosted the AI Action Summit in Paris in February 2025 to boost AI innovation and to address the ethical, social, and economic implications of AI. Over 1 000 participants from more than 100 countries attended the Summit, representing government leaders, international organisations, the academic and research community, the private sector, and civil society. On a smaller scale, **Czechia** organised a third edition of the annual AI 4 Gov event, which brought together representatives of public authorities, the research and academic sector, and private companies to learn and discuss good practices in implementation of human-centric, trustworthy and ethical AI systems in public administration.

> **Best practice**
>
> **Austria** has launched the AI Advisory Board in 2024 to advise the Federal Government on the implementation of the AI Act and how to use the opportunities that AI offers. The aim is to leverage economic potential, provide support to politicians with AI-related questions and, overall, bundle knowledge about AI. The Board consists of 11 experts from the academic sphere and business who are experts in the fields of ethics, research, economics, law or technology. Austria has also established an AI Service Desk under the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR), which serves as a central point of contact for citizens, organisations, and companies, offering support with questions on implementation of the EU AI Act.

A fair digital environment

The Declaration provides that everyone should be able to effectively and freely choose which online services to use, based on objective, transparent, easily accessible and reliable information. The signatories committed to ensuring a safe and secure digital environment based on fair competition, where users' fundamental rights and consumer protection is in place, and the responsibilities of platforms, especially large players and gatekeepers, are well defined.

EU action

The **Digital Services Act (DSA)** is the EU's primary framework for **ensuring a fair digital environment** *(11a)* and increasing online safety and protecting the fundamental rights of users in the EU. It empowers users and civil society to better understand how the online platforms they are using function and to contribute to making these online platforms safer, more trustworthy and more pleasant.

The DSA became fully applicable in February 2024 and applies to all online intermediaries which offer services to recipients that have their place of establishment in the EU or are located here. Member States had until February 2024 to appoint and empower their Digital Services Coordinators (DSCs), which are independent regulators that work with each other and the Commission to ensure the correct application of the DSA in their Member States. Since February 2024, The DSCs have met in the context of the **European**

Board for Digital Services, chaired by the Commission. The DSA Board contributes to the consistent application of the DSA and the effective cooperation of the DSCs and the Commission. It also contributes to guidelines and analysis of emerging issues across the internal market and assists in the supervision of very large online platforms and very large online search engines.

The Commission has opened infringements proceedings against a number of Member States which have failed to designate and fully empower their DSCs. At time of publication, Poland had not yet designated a Digital Services Coordinator, and five Member States had not fully empowered their designated Coordinators: Czechia, Cyprus, Spain, Poland and Portugal.

Under the DSA, very large online platforms are obliged to assess and mitigate risks related to the dissemination of illegal content, disinformation, gender-based violence, and any negative effects on the exercise of fundamental rights, enshrined in the charter, including freedom of expression, rights of the child, public security and mental well-being.

At the same time, the DSA has introduced unprecedented transparency obligations regarding content moderation practices. It protects EU users against the removal of lawful content. In the course of DSA enforcement, the Commission has already opened formal proceedings against specific platforms, namely against X (December 2023), three against TikTok (February, April and December 2024), AliExpress (March 2024), two each against Meta's Facebook and Instagram (April and May 2024), and against Temu (October 2024) because of potential breaches of the DSA, including in respect of obligations on risk assessments and mitigation measures with regard to the spread of illegal content and disinformation, protection of minors, complaint handling mechanism, transparency requirements, content moderation, advertising transparency, data access for researchers, deceptive advertising and political content, illegal sale of products, recommender systems and addictive design. In May 2025, the Commission initiated formal proceedings against Pornhub, Stripchat, XNXX, and XVideos for suspected breaches regarding protection of minors. As enforcer of the DSA with regard to very large online platforms, the Commission has sent over 100 requests for information related to enforcement priorities, including on the spread of illegal content and disinformation, to assess DSA compliance.

The **Digital Markets Act (DMA)** is applicable since May 2023. Following the first designations of gatekeepers in September 2023, these gatekeepers where then required to meet the obligations set by the DMA in March 2024[21]. It is designed to protect contestability and fairness in digital markets and thereby enable innovation and choice. It does so by means of clearly defined obligations applicable to designated gatekeepers. The DMA aims to tackle practices that have proven to be harmful for businesses and consumers in the past, e.g., based on competition law enforcement; market studies or investigations [22]. Each gatekeeper needs to provide the Commission with a report describing in a detailed and transparent manner the measures it has implemented to ensure compliance with the DMA

---

[21] On 6 September 2023 the European Commission designated for the first time six gatekeepers - Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft - under the Digital Markets Act (DMA). On 13 May 2024, the Commission added Booking to the list of gatekeepers. A total of 23 core platform services provided by those seven gatekeepers are currently designated.
[22] The Commission publishes annual DMA reports, which describe the measures taken to ensure the effective enforcement of the DMA. In April 2025, the Commission published its second report on DMA implementation, which is available at: https://digital-markets-act.ec.europa.eu/commission-publishes-annual-report-dma-implementation-2024-2025-04-25_en.

obligations. They also need to publish a non-confidential summary of such a report as of 7 March 2024. Both the report and the non-confidential summary must be updated at least annually.

In April 2025, the Commission found Apple and Meta in breach of the DMA and fined them EUR 500 million and EUR 200 million respectively. In particular, the Commission found that Apple had failed to comply with the obligation to allow app developers distributing their apps via Apple's App Store to inform customers, free of charge, of alternative offers outside the App Store, steer them to those offers and allow them to make purchases. The Commission also found that Meta's 'consent or pay' model is not compliant with the DMA, as it did not give users the required specific choice to opt for a service that uses less of their personal data but is otherwise equivalent to the 'personalised ads' service. The two decisions came after extensive dialogue with the companies concerned, allowing them to present in detail their views and arguments.

In the area of **consumer protection**, the Commission presented the conclusions of its comprehensive **Fitness Check of EU consumer law on digital fairness** on 3 October 2024. The Fitness Check assessed how well EU consumer protection instruments are continuing to ensure fairness for consumers in the digital world. It concluded that, while the EU's consumer protection regulatory framework remains relevant and compliance costs are moderate, its objectives of a high level of consumer protection are being only partly achieved in the digital environment. The current – largely principle-based – consumer rules in the complex digital area are being ineffectively enforced. This significantly disadvantages consumers in the online sector and creates legal uncertainty for the traders about how to apply them. The Fitness Check therefore specifically identified several gaps of consumer protection.

The Commission has started preparing a proposal for a Digital Fairness Act (DFA) that is expected to be presented in the second half of 2026 (see the Mission Letter to Commissioner McGrath). The DFA will specify the current largely principle-based consumer protection rules and thus address the problems identified in the Fitness Check. These could include dark patterns on online interfaces that can unfairly influence consumer decisions, or addictive design features that stimulate consumers to keep using the service or spend more money. Stronger protection of minors online will be a transversal priority for the Commission in these areas. The DFA could also tackle contractual problems (e.g. difficulties in cancelling contracts that have been concluded online) and unwanted contract extensions and conversions of free trials into paid subscriptions. The DFA will not duplicate rules that already exist (for instance in the DSA). It will, however, include a strong simplification and burden reduction element in the areas identified in the Fitness Check, but without compromising the overall objective of high level of consumer protection.

As regards influencer marketing, in 2024, the Commission and national consumer protection authorities of 22 Member States, Norway and Iceland published the results of a sweep of social media posts from 576 influencers [3]. This found that, although nearly all influencers (97%) posted commercial content, **just 20% of influencers systematically indicated the commercial nature of the content shared**. In the consumer survey for the Fitness Check, 74% of consumers reported a lack of transparency regarding paid promotions by social media influencers. 60% of the consumer respondents in the 2025 Consumer Conditions Scoreboard survey echoed these concerns.

The Scoreboard found that online shoppers are over 60% more likely to experience problems with their purchases than those shopping offline. 93% of online shoppers worry about online targeted advertising (including the collection of personal data, excessive advertising and personalisation). 45% of consumers

encountered online scams and many experienced unfair practices (including fake reviews and misleading discounting).

The EU and Member States have also undertaken in the Declaration to promote **interoperability, transparency, open technologies and standards** in order to further strengthen trust in technology as well as consumers' ability to make autonomous and informed choices (*11b*).

The **EU Data Act** entered into force on 11 January 2024 and will be applicable as from 12 September 2025. The Data Act gives both professional and individual users of connected products the right to port personal and non-personal data generated by such products to service-providers of their choice – in full respect of the rights of other data subjects and, to a certain extent, in respect of the interests of a company to preserve its trade secrets.

The **Data Act's** cloud-switching provisions aim to empower cloud customers to choose their cloud-provider freely or combine multiple providers in a multi-cloud deployment. To this end, the Data Act tackles lock-in practices that providers have been using to prevent their customers from switching. Individual provisions (such as the obligation for cloud service providers to reduce switching and egress charges to the costs incurred) are already in application. Most of the Data Act's provisions will apply as from 12 September 2025.

EU policy on the cloud aims to ensure that customers have freedom of choice in a competitive market structure. The Commission is undertaking several actions to pave the way for the effective implementation of the Data Act's provisions on cloud switching. With a view to boosting the interoperability of cloud services, the Commission has launched a study to build a central Union repository for the interoperability of data processing services, which will contain both harmonised standards and industry-driven open interoperability specifications. Moreover, the Commission has launched a study to collect data on whether the gradual withdrawal of switching and egress charges (as provided for in Article 29 of the Data Act) is having an impact on the market.

The Commission is preparing a recommendation on voluntary, non-binding model contractual terms for the implementation of the new portability right and non-binding standard contractual clauses as a voluntary compliance tool for the Data Act's cloud provisions. These models will be based on a Report of an expert group[23]. The recommendation will be published in 2025. The Commission is publishing regularly updated frequently asked questions on the Data Act[24].

In the context of **data spaces**, the Data Act (Article 33), which incorporates the FAIR principles to ensure the findability, accessibility, interoperability and reusability of shared data, calls for the development of harmonised standards to address essential interoperability requirements. The requirements aim to facilitate automation of data transactions by defining cross-domain standards for metadata and trust mechanisms. One of the top priorities of the Annual Union Work Programmes on European Standardisation 2024 and 2025 is the establishment of a European Trusted Data Framework. Based on this, a standardisation request has been developed which is expected to be adopted in Q2 2025. In the meantime, European standardisation organisations (e.g. the European Committee for Standardisation

---

[23] https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3840
[24] https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act

(CEN) and the European Telecommunications Standards Institute (ETSI)) have established technical committees that will carry out the work.

The **European Data Innovation Board** (a Commission expert group that was first established under the Data Governance Act) is also responsible for ensuring the consistent application of the Data Act.

Member State action

In 2024, the Member States continued to implement initiatives to support a fair digital environment, including by supporting EU businesses. For instance, **Luxembourg** continued to implement its roadmap for developing the start-up ecosystem.

When it comes to consumer protection, the international cooperation between Nordic consumer protection authorities (Denmark, Finland, Iceland, Norway and Sweden) is worth noting. It met in August 2024 to discuss new consumer challenges posed by digitalisation, major global players, e-commerce and cross-border marketing. They recognised the need for cross-border cooperation (building on similar consumer protection regulations) to prevent and end illegal marketing practices and unfair contract terms in the Nordic region. The authorities agreed to continue issuing joint statements, pool their resources in joint enforcement cases and share best practices. *(11a)*

In order to strengthen trust in technology, measures to support transparency such as the one below provide a good example. *(11b)*

> **Best practice**
>
> In **Portugal**, the city of Porto together with Porto Digital and Helpful Places put forward the Digital Transparency in Porto pilot project in 2024. The pilot aims to enhance transparency by giving citizens access to data on the technologies that shape the city. It combines physical signage with a digital platform, making it easier for residents and visitors to access information about urban technologies and services (e.g. weather stations, traffic CCTV cameras and Wi-Fi access points). Each sign features icons that indicate the type of technology and the responsible organisation; and a QR code that links to Porto City's Digital Systems Information Platform, where users can find detailed information about data collection and processing. Overall, the project reinforces Porto's commitment to data transparency, empowering citizens to understand and actively participate in the urban digital ecosystem.

Chapter IV - Participation in the digital public space

Besides recalling the right to freedom of expression and information as well as freedom of assembly and of association in the digital environment, the Declaration includes a number of principles and commitments on access to a trustworthy, diverse and multilingual digital environment, with a view to contributing to a pluralistic public debate and to effective and non-discriminatory participation in democracy. It particularly highlights the role of online platforms in mitigating the risks stemming from the use of their services in relation to disinformation, which is now also the object of a legal obligation for VLOPs and VLOSEs under the DSA. These latter platforms and search engines are required to assess and mitigate the risks that their services or systems might pose to electoral processes or civic integrity. This commitment is closely linked with the digital decade's general objective of promoting a digital environment that fosters democratic life, is human-centred and fully respects fundamental rights.

According to the 2025 Eurobarometer[25], **a stable majority continues to think that the freedom of expression and information online (e.g. via online platforms, social networks or search engines) is well protected in their Member States** (60%, similarly to previous years), as well as their right to freedom of assembly and association in the digital environment (59%, similarly to previous years).

Over half of EU citizens (53%) believe that they have access to a trustworthy, diverse and multilingual digital environment, including more diverse content, less disinformation and less illegal content (53%, the same as in 2024). The most positive views come from Luxembourg (75%), followed by Croatia (69%).

Worryingly, one third (33%) of EU citizens continue to think that they cannot rely on the information they see online (35% in 2024). This is especially the case in Greece (49%) and Slovakia (40%), where citizens' negative views rose during the year (+5% on average). In the Netherlands (39%), Germany, Spain and Sweden (38% in all three), citizens remain critical but were slightly less worried than last year.

Based on the impact indicator framework developed by the support study[26], taking into account both available data and perceptions of citizens, **the commitments in this chapter are estimated to be only 56% implemented** (2023 data). The indicators suggest that Member State action in this area has the second least effective impact on the ground among all Declaration chapters. Particularly large gaps have been reported in Germany, Greece, Portugal and Slovakia, where the impact of these initiatives appears to be below 50%. It is worth adding that this estimation takes into account available EU-27 data, which, in this case cover only three of the six the commitments in this chapter.

EU action

The EU has made a commitment to continue safeguarding all fundamental rights online and particularly the freedom of expression and information (including **media freedom and pluralism**) *(15a)*.

The [European Media Freedom Act (EMFA)](#), which was adopted in April 2024, has established a new set of rules to protect media pluralism and independence in the EU. The provisions on the new European Board for Media Services [27] came into force on 8 April 2025. The new media board is composed of representatives from the national media authorities or bodies and is assisted by a Commission secretariat. It started operating in February 2025 and will as part of its work promote the effective and consistent application of the EU's media law framework.

The EU and its Member States have made a commitment in the Declaration to support the development and best use of **digital technologies to stimulate people's engagement and democratic participation** (*15b)*.

The December 2023 [Commission Recommendation](#) **on inclusive and resilient electoral processes** provided a comprehensive blueprint to support the preparations for and conduct of elections. For example, it encourages Member States to take measures to protect the information environment around elections and ensure that voters receive correct information. It recommends building resilience and

---

[25] 2025 Special Eurobarometer Report on the Digital Decade, available here: https://digital-strategy.ec.europa.eu/en/news-redirect/883227

[26] Study to support the monitoring of the Declaration on Digital Rights and Principles, available here: https://digital-strategy.ec.europa.eu/en/news-redirect/883230

[27] The new board replaced and succeeded the European Regulators Group for Audiovisual Media Services (ERGA) that had been established under the Audiovisual Media Services Directive.

developing public awareness, media literacy and critical thinking to address information manipulation, interference and disinformation related to elections. It also calls on Member States to develop training to relevant authorities and to facilitate cooperation among relevant stakeholders to tackle the information manipulation risks.

The Recommendation encourages political parties to adopt campaign pledges and codes of conduct on election integrity and fair campaigning. Such codes should encompass for example the pledge to encourage an inclusive political discourse, or the pledge to refrain from manipulative behaviour, in particular producing, using or disseminating falsified, fabricated, doxed or stolen data or material, including deep fakes generated by AI systems. Political parties should also provide information about the use of AI systems in election campaigns.

Based on this Recommendation, all European political parties signed a **Code of Conduct** for the 2024 European Parliament elections at a ceremony hosted by the Commission[28]. The Code was also signed by a limited number of national political parties. The Code of Conduct promotes core values such as transparency, fairness, and truthfulness in communication, while actively countering disinformation and AI-driven manipulation.

The Commission has committed to adopt in June 2025 an extensive Report to the European Parliament setting out the wide range of actions taken in the context of the 2024 European Parliament elections.

In 2024, the Commission continued to support Member State authorities in the context of the European Cooperation Network on Elections. This Network, which consists of national contact points appointed by Member States to represent their national networks on elections serves as a liaison point between national and European levels of coordination and regularly meets to share best practices.

In April 2024, the Commission issued **guidelines** for the Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs) on the measures they have to take to mitigate threats to **electoral integrity**. The Commission works closely with the Member States' digital services coordinators, both in the European Board for Digital Services and directly with the authorities of those Member States which have upcoming elections.

The EU is also taking measures to tackle illegal and harmful content online, in full respect for fundamental rights, including the right to freedom of expression and information. In coordination with specific measures outlined in EU legislation such as the Terrorist Content Online Regulation or the recently adopted EU directive on combating violence against women which criminalises cyberviolence, the EU is implementing groundbreaking horizontal rules to tackle illegal content through the DSA (*15c*).

Online platforms have to put systems in place for users in the EU to flag illegal content (e.g. terrorist content, child sexual abuse material and illegal hate speech). The DSA requires online platforms to have an easily accessible and efficient point-of-contact for users, as well as a notice-and-action mechanism that allows users to report illegal content. The DSA applies a risk-based approach with specific obligations and direct Commission oversight of platforms that reach at least 45 million EU users a month.

---

[28] International Idea, CODE OF CONDUCT FOR THE 2024 EUROPEAN PARLIAMENT ELECTIONS, 04 April 2024.

Such VLOPs also have a broader due diligence obligation to effectively mitigate systemic societal risks in the EU (e.g. election manipulation, gender-based cyber violence and online harm to minors). The platforms have to implement their own terms of service diligently and non-arbitrarily.

Freedom of expression lies at the heart of the **DSA**. It sets out rules for online intermediaries to tackle illegal content, while safeguarding freedom of expression and information online. The DSA does not require online intermediaries to remove lawful content, but it does require VLOPs and VLOSEs to establish a robust mechanism (a notice-and-action system) where any European can report content that they believe to be illegal hate speech under EU or Member State law. The DSA does not define illegal hate speech. At EU level, the 2008 **Framework Decision on combating racism and xenophobia** provides a baseline, but Member States may go beyond this. Indeed, 20 Member States have expanded their criminal law framework to include additional grounds, such as sexual orientation, gender identity or disability. This will be complemented by the transposition into national law of the 2024 Directive on combating violence against women, which states that cyber incitement to violence or hatred on grounds of gender is a criminal offence.

The DSA also requires VLOPs to take effective measures to mitigate risks related to the dissemination of illegal content, gender-based violence and fundamental rights, including the right to freedom of expression and information and the right to non-discrimination.

On 20 January 2025, the Commission and the European Board for Digital Services integrated the revised **code of conduct on countering illegal hate speech online+** (the Code of Conduct+) into the regulatory framework of Article 45 of the Digital Services Act (DSA). The Code of Conduct+ has been signed by Dailymotion, Facebook, Instagram, Jeuxvideo.com, LinkedIn, Microsoft, Snapchat, Rakuten Viber, TikTok, Twitch, X and YouTube. It aims to strengthen the way that online platforms deal with content that is deemed to be illegal hate speech according to EU law and Member States' laws. Adherence to the Code of Conduct+ may be considered as an appropriate risk-mitigation measure for signatories designated as VLOPs and VLOSEs under the DSA. The Code of Conduct+ also increases transparency and accountability, because compliance with its commitments will be subject to an annual independent audit which these service providers must undergo under the DSA.

In April and May 2024, the Commission organised a **European Citizens Panel on tackling hatred in society**, bringing together 150 randomly selected citizens from all 27 Member States to discuss the root causes and drivers of hatred, and ways to address them. The Panel agreed on 21 recommendations [29] to the Commission and Member States. Several of these recommendations focus on the challenges and responses concerning the digital dimension of hate.

The DSA also aims to tackle content that is harmful but not necessarily illegal, such as **disinformation** and information manipulation and other forms of **harmful content** (including harassment and gender-based violence) (*15d*).

The Digital Services Act fosters a co-regulatory framework. Following a request by the signatories of the Code of Practice on Disinformation, the European Board for Digital Services and the Commission adopted positive opinions on its conversion into a **DSA Code of Conduct** in February 2025. At the signatories'

---

[29] The full list of recommendations is available on the citizens' panel web page: https://citizens.ec.europa.eu/european-citizens-panels/tackling-hatred-society-panel_en.

request, the legal effects of the conversion will enter into force on 1 July 2025. From this point onwards, the commitments made by the signatories designated as VLOPs and VLOSEs will be regularly audited.

The Code of Conduct contains a broad range of commitments made by major online platforms and other players to fight disinformation with measures such as demonetisation, addressing manipulative behaviours, user empowerment and fact-checking. A substantial number and great variety of new signatories – 42 to date – have signed the Code, including major online platforms (e.g. Google, Meta, Microsoft and TikTok). The signatories have also taken action to help safeguard the integrity of the 2024 European elections. In particular, they implemented have established a **Rapid Response System** for elections, which allows civil society and fact-checker signatories to swiftly report time-sensitive content, accounts or trends that they view as threats to the integrity of the electoral process. The signatories have also used this system for the French, Romanian and German elections.

The Code of Conduct will play an important role in the wider system of enforcement under the DSA, contributing to its practical application, and particularly serving as a relevant benchmark for DSA implementation when it comes to risks related to disinformation

One of the main regulatory tools of the DSA is the supervised risk management framework for VLOPs and VLOSEs. Their size means that they can have important impacts on our societies.

The risk management framework requires these platforms to regularly assess and effectively mitigate systemic risks. For instance, if their content moderation tools or recommender systems are found to be amplifying disinformation, they must take appropriate measures to address risks that can have a negative effect on their users. The platforms will also have to report publicly on their risk assessment and risk mitigation measures, and these will be audited by independent auditors and supervised by the Commission.

In addition, VLOPs and VLOSEs have to provide researchers with access to data and study risks in the EU (including those related to disinformation). This will be a step change in our understanding of the online information space and the way that disinformation spreads online.

The EU is also funding the **European Digital Media Observatory (EDMO)** and its national and regional hubs, which support the creation of a cross-border and multidisciplinary community of independent fact-checkers and academic researchers that are working together to detect, analyse and expose potential disinformation threats and raise media literacy. EDMO comprises a network of 14 national and multinational hubs covering all 27 EU Member States. The hubs' local knowledge allows EDMO to strengthen detection and analysis of disinformation campaigns, improve public awareness and design effective responses for national audiences across the EU. For the 2024 European Parliament elections, EDMO established a dedicated taskforce to monitor the EU's information space. It issued daily briefs and early warnings about disinformation narratives, and ran an EU-wide 'BeElectionSmart' media literacy campaign. The taskforce was assisted by a pool of AI experts to swiftly detect and expose deceptive or misleading AI-generated content. EDMO has also continued to publish monthly updates on the disinformation situation in the EU and worked to counter disinformation concerning Russia's illegal invasion of Ukraine.

The Declaration also contains a commitment to support **effective access to digital content that reflects the EU's cultural and linguistic diversity**. The **common European data space for cultural heritage** is a

flagship initiative to accelerate the digital transformation of the cultural heritage sector, building on the work of the European Initiative. It features access to diverse content (including digitised cultural heritage objects, editorials and other resources) related to diversity and inclusion. These range from content and exhibitions on under-represented cultures or cross-cultural exchange[30] to resources on women's history[31] to promoting a more inclusive and respectful approach to describing digital collections[32] (*15e*).

The Commission is preparing the **new European Democracy Shield**, which will provide a strategic approach to safeguard and strengthen democracy in the EU during this mandate, aiming to reinforce public trust in democracy and democratic institutions, to increase democratic resilience and to react to evolving challenges. A **call for evidence** asking for feedback as well as a **public consultation** were launched in March 2025.

Member State action

Overall, 239 Member State initiatives related to the implementation of a trustworthy and diverse digital environment (*chapter IV*) were identified by the support study, showing a **rather low level of activity in this area**. That said, with citizens' call for a more trustworthy digital environment, **activity is increasing**. In 2024, 146 initiatives were launched, making it the highest number of initiatives in this area in recent years.

Efforts mostly contribute to supporting the development and best use of digital technologies to stimulate people's engagement and democratic participation *(15b)*, while the fewest number of initiatives have been identified with regards to empowering individuals to make freely given, specific choices and limiting the exploitation of vulnerabilities and biases, namely through targeted advertising *(15f)*.

Most initiatives are led by government organisations (77%), supported by activities originated by civil society, industry and National Human Rights Institutions. Initiatives are predominantly research and technology solutions (22%), as well as policy related (18%) or legislative (17%). While the majority of initiatives is put forward at national level (70%), relatively many actions taking place at international (14%) and regional/local level (17%).

In 2024, several Member States implemented measures to tackle illegal and harmful content online. The Centre for Social Informatics (CSI) and the Peace Institute in **Slovenia** have, for instance, launched a new project that aims to analyse the perception of hate speech and disinformation through an online survey and develop a corresponding proposal for action.

In **Latvia**, a one-year project, on monitoring and reporting for a safer online environment, funded by the EU CERV programme, sought to apply a comprehensive and intersectional approach in preventing intolerance, racism and xenophobia online. The European Digital Media Observatory has also supported Member States in detecting and analysing disinformation, training professionals and citizens as well as providing support to authorities in monitoring online platforms. There are currently 14 operational hubs active in all Member States and Norway. (*15c,15d,15f)*

---

[30] Cf. https://www.europeana.eu/en/inclusion-and-diversity-through-citizenship

[31] Cf. https://pro.europeana.eu/tags/womens-history-month

[32] Cf. https://pro.europeana.eu/page/the-de-bias-vocabulary; https://op.europa.eu/en/web/eu-vocabularies/dataset/-/resource?uri=http://publications.europa.eu/resource/dataset/de-bias-ontology

To further empower citizens online, **Sweden** has launched Källkritikbyrån, a project to help people become confident and conscious internet users. It provides inspiration and knowledge to become more critical of online sources. The project systematically reviews online claims and passes on the knowledge to the general public.

In 2024 **Hungary** established a national register of advertising devices. This initiative aims to ensure that all advertising tools comply with urban landscape protection regulations. Owners of advertising devices must register their tools so that their devices are allowed. *(15a, 15f)*

When it comes to the use of digital technologies to stimulate people's engagement and democratic participation, **Cyprus** has launched an online platform Citizen's Voice which provides citizens with the possibility of two-way communication with the government. As part of participatory democracy, via the 'Citizen's Voice' portal, the government conducts citizens' advisory votes on major issues concerning legislation and policies it intends to implement. *(15b)*

To support access to digital content reflecting cultural and linguistic diversity, **Finland**'s National Digital Library Finna continued to provide access to a wide range of digital cultural heritage materials, including documents, photographs, and audiovisual recordings, in multiple languages. *(15e)*

Further national efforts may be expected following the implementation of the Digital Services Act and the European Media Freedom Act.

Best practice

Luxembourg has been active in raising awareness about safe and responsible use of digital technology, particularly among children and young people. In 2024, its governmental initiative BEESECURE delivered 1 127 digital literacy training sessions, mainly to children and young people in schools but also parents, teachers and others. A campaign launched in 2024 aimed to raise awareness about how AI-generated content, especially deep fakes, could mislead the public and spread disinformation.

BEE SECURE also includes an anonymous reporting platform Stopline where users can report illegal content such as child sexual abuse material, racism and hate speech. Relevant content is forwarded to the national police or other authorities.

BEE SECURE is co-funded by the EU and part of the European networks Insafe (awareness-raising centres and helplines) and INHOPE (International Association of Internet Hotlines, reporting centres for illegal content).

Chapter V - Safety, security and empowerment

In keeping with the objective of protection against cyberattacks in the Digital decade, the signatories to the Declaration committed to take (further) measures to promote traceable and safe products on the Digital Single Market, and to protect people, businesses and public institutions against cybersecurity risks and cybercrime, including via cybersecurity requirements for connected products placed on the single market.

Overall, 530 Member State initiatives on the implementation of a safe and secure digital environment (*chapter III*) had been identified by the support study[33] by the end of 2024. The highest number of initiatives focus on the *section A protected, safe and secure digital environment (Chapter V),* concretely on protecting the interests of people, businesses and public institutions against cybersecurity risks and cybercrime, including data breaches and identity theft and manipulation (*16b*).

The majority of initiatives are led by government organisations (73%), with reasonably strong support from civil society (16%), industry (7%) and national human rights institutions. Initiatives are predominantly policy related (24%), and popular measures include training courses and educational initiatives (18%) as well communication-related initiatives (17%), complemented by quite a few harmonisation initiatives, such as guidelines and certification schemes (8%). Although most initiatives are at national level (84%), action in this area is supported by city initiatives (6%).

Based on the impact indicator framework developed by the support study, taking into account both available data and public perceptions, **the commitments in this chapter are estimated to be implemented at 54%** (2023 data), making it the least implemented chapter of the Declaration. **Despite relative activity of Member States in this area**, the impact indicators suggest that **Member States are struggling to ensure effective impact of these measures on the ground**. This is true in particular in 8 Member States, where the impact is estimated to be equal or below 50%: Belgium, Bulgaria, Germany, Greece, France, Romania, Slovakia and Sweden[34].

A protected, safe and secure digital environment

According to the 2025 Eurobarometer[35], **a majority of Europeans (55%) consider that they have access to safe and privacy-friendly digital technologies in their country** (same as in 2024 and 2023), especially in Finland (76%) and Malta (71%). Similarly to previous years, one third (33%) remains of the opposite view however, with most critical citizens in Greece (51%), Spain (41%) and Slovakia (40%).

EU action

The **Digital Services Act (DSA)** sets EU-wide rules for online intermediaries, including for online marketplaces that connect sellers with consumers. The rules seek to ensure that traders can only sell products on online marketplaces that are compliant with the relevant product safety and other requirements *(16a)*.

Online marketplaces have an obligation to counter illegal goods offered through their service. This implies, for example: the obligation to put in place user-friendly notice-and-action and complaint handling mechanisms; a duty of cooperation with trusted flaggers; a ban on dark patterns; rules on advertising, and detailed transparency obligations, including how products are recommended to consumers.

---

[33] Study to support the monitoring of the Declaration on Digital Rights and Principles, available here: https://digital-strategy.ec.europa.eu/en/news-redirect/883230

[34] This estimation takes into account available EU data, in this case covering only 7/12 commitments in this chapter. The main gaps in data availability concern the section Protection and empowerment of children and young people in the digital environment, where only 2/5 commitments have a data source.

[35] 2025 Special Eurobarometer Report on the Digital Decade, available here: https://digital-strategy.ec.europa.eu/en/news-redirect/883227

Online marketplaces also have to comply with the 'know your business customer' obligation that require them to gather certain information about traders before they offer their products on the platform. Information includes for example the identity and contact details of the trader, information on their payment account, their trade registration details, and a self-certification committing them to only offer products that comply with EU rules, and online marketplaces should make best efforts to assess whether the information is reliable and complete.

The **General Product Safety Regulation (GPSR) applicable from 13 December 2024 (see also here)** introduced specific product safety-related obligations for providers of online marketplaces, building on the general framework of the DSA. For example, providers of online marketplaces that target EU consumers need to register with the EU Safety Gate Portal and indicate their point of single contact there. The GPSR also introduced strict deadlines for handling governmental orders and notices and specified the minimum information that need to be indicated by traders on each product listing, before their publication on online marketplaces.

The GPSR also introduced new enforcement mechanisms in the area of product safety. For example, national market surveillance authorities of the Consumer Safety Network will now be able to conduct simultaneous compliance checks, 'product safety sweeps', which are particularly relevant and effective in online worlds.

In the **E-Commerce Communication** adopted in February 2025, the Commission promotes digital solutions like the **Digital Product Passport (DPP)** as a key enabler for the supervision of the e-commerce landscape, supporting authorities by making available product regulatory compliance information available in a digital format. Over time, most physical goods placed on the EU market or put into service will require a DPP. Enhancing the transparency of product specific information will enable consumers, manufacturers and authorities to make more informed decisions.

The Commission is prioritising the effective implementation of the DPP as well as expanding its scope for regulatory compliance, in proposals like the Toy Safety Regulation, the Detergents and Surfactants Regulation or the Green Claims Directive. It aims to extend the use of the DPP system to other policy areas, promoting it as a single entry point for all product-specific information, such as instructions, declaration of conformity and conformity certificates. In line with these efforts, the Commission announced measures to support a modern and resilient supervisory toolbox, in particular through the use of the DPP for detecting illegal goods, and shared databases.

Additionally, the DPP, together with the EU Single Window Environment for Customs and later the EU Customs Data Hub, will also simplify the work of customs authorities, market surveillance authorities, and economic operators when a product enters the EU market. Therefore, customs authorities will be able to use the information made available through the DPP for risk management purposes to more efficiently allocate their resources to the most relevant tasks.

The signatories of the Declaration also committed to protecting the interests of people, businesses and public institutions against cybersecurity risks and cybercrime, including data breaches and identity theft and manipulation. This includes cybersecurity requirements for connected products placed on the single market *(16b)*.

The EU has developed a strong framework to ensure the security and resilience of our critical infrastructure. One example is the **5G Toolbox** which provides recommendations to ensure that 5G networks are secure and resilient. However, the state of implementation of the 5G Toolbox by Member States is not complete, as many Member States still do not have restrictions on high-risk suppliers. This creates a significant risk of strategic dependency on high-risk suppliers and our EU 5G networks being subject to interference from countries outside the EU.

Building on the 5G Toolbox, Member States, together with the Commission and the EU Agency for Cybersecurity, carried out a risk assessment on the cybersecurity and resilience on Europe's communications infrastructure.

Regarding the **security of supply chains,** the Commission and ENISA, through the NIS Cooperation Group, are conducting risk assessments of specific critical ICT services, ICT systems and ICT products supply chains, recommending mitigation measures to ensure their security.

Member States had to transpose the **Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)** into national law by 17 October 2024. This Directive aims to ensure a high level of cybersecurity across the EU. It covers entities operating in sectors that are critical for the economy and society, including providers of public electronic communications services, ICT service management, digital services, wastewater and waste management, space, health, energy, transport, manufacturing of critical products, postal and courier services and public administration.

In October 2023 the Commission adopted the first implementing rules on cybersecurity of critical entities and networks under the NIS2 Directive. This implementing act details cybersecurity risk management measures as well as the cases in which an incident should be considered significant and companies providing digital infrastructures and services should report it to national authorities.

The implementing regulation applies to specific categories of companies providing digital services, such as cloud computing service providers, data centre service providers, online marketplaces, online search engines and social networking platforms. For each category of service providers, the implementing act also specifies when an incident is considered significant.

The **Cyber Resilience Act** entered into force on 10 December 2024 and its main obligations will start applying from 11 December 2027. It introduces **cybersecurity requirements for hardware and software** accessing the European market, including support obligations for the time the products are expected to be in use. It forms a crucial pillar of EU's prevention system, tackling the challenges consumers and businesses currently face when trying to determine which products are cybersecure and setting them up securely.

In 2024, the Commission adopted the first **EU cybersecurity certification scheme**, based on Common Criteria (EUCC). A first of its kind, the EUCC will allow suppliers of ICT products and services to showcase the cybersecurity of their offer, as well as to raise awareness and empower businesses and consumers to select more cybersecure products. The scheme started being available for vendors as of February 2025.

The 2024 **Cyber Solidarity Act** entered into force on 4 February 2025. It aims to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents. Under this Regulation, the European Cybersecurity Alert System will be established to build coordinated detection

and situational awareness capabilities, reinforcing the Union's threat detection and information-sharing capabilities. The Regulation also provides for setting up a Cybersecurity Emergency Mechanism to support Member States in preparing for, responding to, mitigating the impact of and initiating recovery from significant cybersecurity incidents and large-scale cybersecurity incidents.

Thirdly, the European Cybersecurity Incident Review Mechanism will be created, to review and assess specific significant cybersecurity incidents and large-scale cybersecurity incidents.

Member State action

In 2024 in **Luxembourg**, the Ministry of the Economy, in close cooperation with the National Cybersecurity Competence Centre (NC3) and with the support of Luxinnovation, launched the first call for projects under the new funding scheme known as the Cybersecurity Innovation & Development Funding Programme (LU-CID-FP). This call for funding is co-financed by the EU. This initiative aims to bolster the development and adoption of cybersecurity innovations by supporting SMEs and start-ups within Luxembourg. Successful applications to this call will be funded through the Research and Development funding scheme managed by the Ministry of Economy.

To raise awareness about cyber security among both individuals and companies and strengthen their ability to protect themselves against crime, **Sweden** organised an awareness raising campaign 'Tänk Säkert', carried out by the Swedish Civil Contingencies Authority and the Swedish police.

In the meantime, **Estonia** continued to implement its Kübertest, a cybersecurity training and awareness initiative designed to enhance the cybersecurity knowledge and skills of public sector employees. The programme, implemented by RIA (Information System Authority) includes a series of training modules that cover various cybersecurity topics, such as recognising phishing attempts, securing personal and organisational data, and responding to cyber incidents. The training is delivered through an online platform, making it accessible to a wide audience.

> **Best practice**
>
> In 2024, **Malta** launched two funding schemes to support cybersecurity of public and private bodies. First, the CYBER+ALT scheme for SMEs aims to facilitate the implementation of state-of-the-art cybersecurity solutions through cascading of funds. Second, the CYBER ASSESS scheme offers free cybersecurity assessment services to the private and public sector, to assess their cyber resilience.

Privacy and individual control over data

Data protection and privacy are key fundamental rights in the digital age. They are also enabling the protection of other fundamental rights that can be affected by unlawful access, such as human dignity and freedom of expression. The EU and Member States have undertaken to ensure effective control of personal and non-personal data in line with EU data protection rules and other relevant rules, respectively.

They have also committed in the Declaration to effectively protect communications from unauthorised third-party access, prohibiting unlawful identification as well as unlawful retention of activity records. The

EU and Member States also undertook to effectively ensure the possibility for individuals to easily move their personal and non-personal data between different digital services, in line with portability rights.

According to the 2025 Eurobarometer survey[36], **only a slight majority of Europeans consider that their privacy online** (i.e. respect for the confidentiality of communications and information on devices) is well protected (52%, similar to recent years). The most optimistic views are in Malta (73%) and Finland (70%). Worryingly, over one third (36%) of Europeans continue to believe that their privacy online is not well protected, with an alarming majority of citizens in Greece (57%, +6 pp compared to 2024), followed by Spain (44%) and Slovakia (43%, +6 pp).

In addition, only a minority of Europeans believe they have control over their own data, including how it is used online and with whom it is shared (48%, similar to last years). Four in ten Europeans believe their data is not in their control (41%, similar to previous years). The majority of citizens in Greece (57%) and Sweden (53%) are worried about their data. On the positive side, the data also show that individuals are increasingly familiar with and actively exercise their rights under the General Data Protection Regulation (GDPR).

Only four in ten Europeans believe that they are getting control of their digital legacy, for instance deciding what happens with personal accounts and information after they die (42%, comparable to recent years). Equally, almost four in ten Europeans feel they do not have control over their digital legacy (38%).

EU action

The **General Data Protection Regulation (GDPR**) is one of the cornerstones of the EU's approach to digital transformation and ensures that individuals remain in control. Its basic principles - fair, safe and transparent processing of personal data, legitimacy of purpose of processing, data minimisation, data security- underpin all EU policies involving the processing of personal data (*19a)*.

On 25 July 2024 the Commission published the Second Report on the application of the General Data Protection Regulation[37]. It shows that in the six years since the GDPR 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.

At the same time, further progress should be made in a number of areas in the coming years. In particular, the focus should be on supporting stakeholders' compliance efforts - especially small and medium sized enterprises (SMEs), small operators and researchers and research organisations, providing clearer and more actionable guidance from the data protection authorities, and achieving a more consistent interpretation and enforcement of the GDPR across the EU.

To that end, the Commission continues to actively support the swift adoption of the proposal on GDPR procedural rules by the EU Council and European Parliament. This proposal aims to clarify key steps in the

---

cross-border enforcement procedure under the one-stop-shop in the GDPR and would provide definitions for key terms. It would lead to a more consistent interpretation and enforcement of the GDPR.

According to the **Data Act**, processing of **non-personal data** coming from connected products is subject to the requirement of a contractual agreement with the lawful user of the connected product.

Under the Data Act, which entered into force in January 2024 and will be applicable as of 12 September 2025, users (both professional and individual users) of connected products will have the right to port personal and nonpersonal data generated by such products to service providers of their choice – limited by the rights of other data subjects and to a certain extent by a company's legitimate interest in preserving its trade secrets *(19b).*

An expert group[38], that first met in September 2022, composed of academic and industry experts, is preparing model contract terms for the implementation of the new portability right. This will form the basis for a Commission recommendation to be published in the course of 2025. The Commission regularly publishes updated frequently asked questions on the Data Act[39].

Under the ePrivacy Directive the provider of a publicly available electronic communications service has the obligation to take appropriate technical and organisational measures to safeguard security of its services and, those measures must ensure that personal data can be accessed only by authorised personnel for legally authorised purposes *(19c).*

According to the Directive, the implemented appropriate technological protection measures must render the data unintelligible to any person who is not authorised to access it. In addition, the Directive also places an obligation on Member States to ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation.

Under the ePrivacy Directive, the provider of a publicly available electronic communications service has the obligation to take appropriate technical and organisational measures that protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure *(19d).*

In addition, the Directive places an obligation on service providers, where calling line identification is offered, to offer the caller user the possibility, using a simple method and free of charge, of preventing their number from being identified, on a per-call basis.

In light of this, the ePrivacy Directive allows Member States to adopt additional necessary, appropriate and proportionate legislative measures to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication systems.

These measures complement and specify the requirements of the GDPR. In the Commission Work Programme 2025, the Commission announced its intention to withdraw the Proposal to amend the e-Privacy Directive, on which the Parliament and Council could not agree, and which has also become

---

[38] https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3840
[39] https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act

outdated in view of recent legislation[40]. The Commission is currently assessing the next steps to take on this issue.

Member State action

In 2024 in **Sweden**, the Swedish Authority for Privacy Protection published several guides on how individuals may exercise their rights in the field of data protection for private citizens. These guides included information on who to contact and how to proceed if a person's data protection has been infringed. The guides include topics such as data protection in healthcare, data protection as a customer, and data protection online.

In **Denmark**, the Digital Self Defense initiative carried out by the PROSA NGO aims to help citizens protect their privacy online by providing a set of easy-to-use tools and guidelines. The initiative includes recommendations to use secure communication apps like Signal, password managers such as Bitwarden, and privacy-focused email services like Protonmail. The initiative also offers advice on using the Tor network for anonymous browsing, blocking tracking cookies with Privacy Badger, and using alternative search engines like DuckDuckGo to avoid data tracking. Additionally, PROSA organises workshops to teach individuals how to use these tools effectively to safeguard their digital privacy.

In **Estonia**, the Data Tracker online tool continued to provide citizens with a clear overview of how their personal data is being used. It offers transparency by logging and displaying all operations performed with individuals' data on the state portal eesti.ee. This service helps increase awareness of the importance of protecting personal data, and assists authorities in clarifying requests related to personal data.

In the meantime, **Malta** started to implement its 2023-2027 Public Administration Data Strategy. The Strategy aims to ensure that good governance of data is at the core of any digital solution or transformation process. It is applicable to all digital data processed within the public administration. Some of the key objectives are to govern and manage data in a holistic manner across government through the definition of standards, guidelines, tools, policies, and procedures; address data protection legal obligations and rights, cybersecurity, data preservation, and archiving requirements; and facilitate data sharing and re-use through a consistent approach in information systems and datasets.

Also, implementation of the Data Act by setting national enforcement bodies is still on-going.

Best practice

In 2024, in **Germany**, the city of Munich drew up a Code on Data Ethics, developed by innovation, data-protection and business experts. The Code highlights central values in the context of data-driven technologies (e.g. AI), namely responsibility, fairness and transparency. Each value and its corresponding dimensions are described in the Code, giving the readers an idea of what each value encompasses. The Code raises awareness of relevant questions in the context of data-driven technologies while highlighting relevant values and guiding people with effective methods to reflect these values in implementation. The Code aims to support trust in the city as a democratic institution.

---

[40] COM(2016)799 final 2016/0400B (COD)

Protection and empowerment of children and young people in the digital environment

The Declaration provides that children and young people should: (i) be empowered to make safe and informed choices and express their creativity in the digital environment; and (ii) have access to age-appropriate materials and services. Children and young people should be able to enjoy these benefits, while being protected in particular from all crimes committed via – or facilitated through – digital technologies. The Declaration includes several commitments in this respect, including on: (i) providing education; (ii) navigating the digital environment; (iii) protecting children and young people from harmful and illegal content, exploitation, manipulation and abuse online; and (iv) involving children and young people in the development of digital policies that concern them.

Protecting children and young people online is a topic that Europeans remain concerned about, as it apparent in the 2025 Eurobarometer survey[41]. **Only 42% of Europeans polled in this survey consider that their country is ensuring a safe digital environment and safe digital content for children and young people, an alarming number despite a slight improvement since the previous year (39%).**

Overall, almost a half of Europeans (48%) are worried about the safety of children online in their country. This is a slight improvement compared with last year (53%). In 12 EU Member States, the majority of citizens is worried, notably in Greece (65%), Sweden (63%) and Slovakia (62%).

Results of a consultation with children on what they need to feel safe done, carried out by the EU's Children's Participation Platform, show that children do not think they are protected enough online, including through built-in protections, like through age verification tools for social media. They want to know more about risks, where to ask for help and how to report dangerous and unsafe situations, bullying or attacks online, and receive this information in a way that is simple, user-friendly and efficient. As a child interviewed during the consultation said: 'Children want to be more educated in order not to be victims on the internet and their data to be stolen'.

EU action

The protection of minors is a priority for the EU, as recalled in the **2024-2029 Political Guidelines**[42] and the May 2024 **Council Conclusions** on the European and international policy agendas on children, youth and children's rights. The EU toolbox on protection and empowerment of minors online includes the **DSA**, the **Audiovisual Media Services Directive (AVMSD)**, and the **Better Internet for Kids strategy (BIK+)**. The **AI Act** adopted in 2024 bans AI systems that exploit children's vulnerabilities and requires additional safeguards for high-risk applications affecting minors.

Under the BIK+, the Commission is aiming for children to acquire the necessary skills to make sound choices and express themselves in the online environment safely and responsibly. Thanks to the EU co-funded network of Safer Internet Centres (SICs) in Member States, the Commission raises awareness on online safety, providing resources in all EU languages and training across the EU.

---

[41] 2025 Special Eurobarometer Report on the Digital Decade, available here: https://digital-strategy.ec.europa.eu/en/news-redirect/883227
[42] https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en

The EU committed in the Declaration to provide opportunities to all children and young people to acquire the necessary **skills and competences**, including media literacy and critical thinking, in order to navigate and engage in the digital environment actively, safely and to make informed choices (*22a*).

In 2024, the network of Safer Internet Centres and the BIK platform reached more than 35 million users, providing them with almost 2 300 new resources. Network resources, including guides and videos, address diverse online opportunities and challenges, including topics such as algorithms, AI, cyberbullying, online harms, media literacy, healthy screen use, digital marketing tactics, and many others.

Safer Internet Day is the annual worldwide campaign under the (BIK+ to promote online safety for children. On Safer Internet Day 2024 almost 19 000 schools and over 17 000 other organisations were involved in SIC actions across Europe alone.

In 2024, the network and the BIK platform also launched the #MediaSmartOnline campaign to spotlight media literacy actions, initiatives, and resources across Europe. The campaign builds on the resources available within the network while maximising the efforts and activities of other stakeholders (including NGOs, government agencies and industry) involved in supporting practices, developing policy and carrying out research into media literacy. The campaign aims to raise awareness of issues such as disinformation and misinformation. It also has the, and more general aim of increasing media literacy skills among children and young people, while also better upskilling those that support them (such as parents, caregivers and teachers).

The network of SICs and the BIK platform also managed the #AdWiseOnline campaign to address the risks that children face online as young consumers. The campaign focuses on in-game marketing tactics (e.g. persuasive design, dark patterns, and loot boxes in video games) to raise awareness of manipulative practices and children's consumer rights by informing parents, guardians, educators, and policymakers about specific manipulative practices in gaming and digital marketing that target children and young people.

With the Digital Services Act (DSA) now in application, the EU promotes positive experiences for children and young people in an **age-appropriate and safe digital environment** *(22b)*.

The protection of minors is also one of the enforcement priorities of the Commission under the DSA. In 2024 the Commission opened four formal **enforcement proceedings** related to minors, one each against Meta's platforms, Facebook and Instagram, and two involving TikTok. One of the proceedings launched against TikTok led to commitments by TikTok not to launch in the EU a task and reward programme as part of its TikTok Lite service due to its addictive features.

The EU is preparing **guidelines under the DSA** to help online platforms ensure a high-level of privacy, safety and security for children using their services. In August and September 2024, the Commission ran a call for evidence for upcoming guidelines on the protection of minors online, which, once adopted, would give advice on how online platforms are to implement high levels of privacy, safety and security for minors online, as required by the DSA (Article 28). The guidelines are expected to be adopted in mid-2025, and will also help with the consistent application of the rules by national authorities responsible for enforcement vis-à-vis platforms below the threshold of 45m active monthly users.

In 2024, the SIC network and the BIK platform created a guide on age verification, available on the BIK platform. The guide includes family-friendly explainers, a report setting out the different types of age verification tools and requirements, and a guide to age verification for digital providers.

The BIK+ strategy supports and complements the implementation of the DSA provisions on protecting minors. That includes support that SICs provide such as: (i) evidence-gathering via regular reporting by helplines and hotlines; (ii) national-level surveys or studies; (iii) an early warning mechanism on online harms occurring in the EU; (iv) consultations of children and young people regarding their experiences and concerns online (organised via national youth panels).

In her Political Guidelines, President van der Leyen announced **an action plan against cyberbullying** to address the growing trend of abusive behaviour online.

The EU has a comprehensive legislative and policy framework to address this topic, including the Digital Services Act (DSA) and the Better Internet for Kids (BIK+) strategy. The EU co-funded network of Safer Internet Centres (SICs) has been set up to provide awareness campaigns, training, and resources on online safety, including cyberbullying.

However, a more effective implementation is needed to ensure the well-being of children. Building on this existing work, the action plan against cyberbullying will ensure a safe online environment for children with targeted initiatives to tackle the issue while promoting digital literacy and awareness-raising efforts. The SIC network will be at core of the action plan, which will also build on existing good practices of tools and services at national level.

The EU also aims to **involve children and young people in the development of digital policies** that concern them *(22d).* In 2024, the network and the BIK platform organised more than 2 100 events involving the participation of young people. More than 750 children across the EU were consulted in 2024 for the first child-led evaluation of the BIK+ strategy, and BIK youth ambassadors were consulted during the development of the Article 28 DSA guidelines on the protection of minors online (they were consulted through a workshop in September 2024 and a focus group in April 2025). In February 2025, BIK youth panellists were consulted together with the Digital Service Coordinators on the future action plan against cyberbullying. In particular, they were consulted on any difficulties they may currently face in reporting cyberbullying.

The **EU Children's Participation Platform** is one of the key deliverables of the EU strategy on the rights of the child, set up in October 2022. The Children's Participation Platform is also a practical way to uphold children's right to have a say, as enshrined in the EU Charter of Fundamental Rights (Article 24) and the United Nations Convention on the Rights of the Child (Article 12). The aim of the Platform is to: (i) involve children in decision-making processes at EU level; (ii) create opportunities for children to experience democratic processes at EU level; and (iii) connect existing child-participation mechanisms at local, national, and EU levels.

Children representing 87 organisations from 24 EU Member States are part of the Platform. All activities of the Platform are co-created with children. Since its setup, the Platform has organised two rounds of consultations with children on what they need to feel safe and on democracy. Children met during the first General Assembly in June 2023 and the 'Create, Plan, Participate' meeting in June 2024. The Platform's work plan for 2025-2026 has been co-planned with children.

To ensure that children access age-appropriate content, the Commission is developing 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 contract to develop the mini-wallet started at the end of January 2025, with a design phase in early 2025, a development phase in spring, and the release of a highly customisable and modular application by summer 2025, ready for localisation and publishing by Member States and technology providers in the app stores.

To support the Commission's efforts and to ensure that the age-verification solutions on the EU market are in line with the GDPR, the European Data Protection Board on 11 February 2025 has issued a statement on Age Assurance[43].

Member State action

In 2024, Member States implemented measures to empower and protect children in the digital environment. In **Spain**, an expert committee of the Ministry of Youth and Childhood also presented its report for the development of a safe digital environment for young people and children. This report includes an analysis and recommendations for the prevention, early detection, and protection against possible violations of the rights of children and young people. The report proposes 107 measures to create safe digital environments.

In **Malta**, the Digital Innovation Authority (MDIA), in collaboration with eSkills Foundation and other entities, organised several educational events in 2024 targeted at strengthening skills and empowering children and young people in the digital environment. For instance, the one-week conference 'Xploring Intelligence - A Bootcamp on Us and Tech' provided a platform to learn about issues such as technology and ethics, deepfakes, machine learning and security online. MDIA has also organised workshops called 'AI Accelerator Skills For Young Women', providing young women with the necessary digital, ethical, and managerial skills to become content creators and to boost creativity and innovation in solving challenges at the community level using AI.

Member States also continued to conduct activities to promote children's digital skills and literacy. For instance, **Estonia** continued to make available its 'Spoofy' educational cybersecurity game designed for children. The game teaches children about internet safety, including recognising online dangers, behaving responsibly online, and understanding the use of smart devices. It is engaging and interactive, making learning about cybersecurity fun and accessible for young users.

Several Member States also organised activities on the occasion of the Safer Internet Day 2024 (and 2025). For instance, **Italy** launched an awareness raising campaign focusing on the use of AI and organised events for around 500 students.

Best practice

In **Spain**, the City of Barcelona carried out a series of debates called 'Growing up between screens', run by the Barcelona City Council and implemented by the team of the Digital and Democracy Innovation Centre. The debates focused on the digital literacy of children and adolescents and understanding and

---

[43] Statement 1/2025 on Age Assurance: edpb_statement_20250211ageassurance_v1-1_en_0.pdf

protecting their digital rights. A parallel project was also launched to develop skills and support community and educational spaces in the implementation and execution of digital literacy and mediation programmes for children, adolescents and families.

Chapter VI – Sustainability

The Declaration promotes digital products and services with a minimum negative impact on the environment and on society, as well as digital solutions with a positive impact on the environment. Moreover, the Declaration provides that access to accurate and easy-to-understand information on environmental impact and energy consumption should be available to everyone. The EU and Member States committed in the Declaration to: (i) incentivising sustainable consumer choices and business models; and (ii) fostering sustainable and responsible corporate behaviour throughout the global value chains of digital products and services, including with a view to combating forced labour.

According to the 2025 Eurobarometer survey[44], **only half of Europeans (50%, the same as in 2024), consider that they have access to digital products and services that minimise damage to the environment and society.** This includes products and services that can be repaired or recycled, and which do not involve forced labour. Moreover, one third of citizens (34%) think they do not have such access (unchanged compared with 2024 and 2023), with this percentage rising to more than half of citizens in the Netherlands (52%).

Similarly, nearly half of Europeans (49%, comparable to last year) believe that they have access to the right information on the environmental impact and energy consumption of digital technologies in their country. In addition, a stable one third of Europeans (36%) continues to think that their access to this information is limited, including more than half of citizens from Sweden (52%) and almost half of the population in Greece (48%) and in the Netherlands (47%).

Based on the impact indicator framework developed by the support study[45], taking into account both available data and perceptions of citizens, **the commitments in this chapter are estimated to be implemented at 61%** (2023 data). Gaps are reported in Belgium, Finland and Slovakia, where the impact of digital rights initiatives on the ground appears to be equal to – or slightly below – 50%. The gap is especially acute in Romania where the impact is 33%. This estimation takes into account available EU-27 data, in this case covering all four of the four commitments in this chapter.

EU action

The **EU Energy Efficiency Directive (EED recast)** mandates that large data centres (above 500 kW capacity) must report on key performance indicators related to energy and water consumption, cooling efficiency, and the use of waste heat. In March 2024, the Commission adopted a Delegated Regulation laying down the key performance indicators which data centre operators must report to a European database by 15 September 2024 pursuant to Article 12 of the Energy Efficiency Directive. The collected data will inform

---

[44] 2025 Special Eurobarometer Report on the Digital Decade, available here: https://digital-strategy.ec.europa.eu/en/news-redirect/883227

[45] Study to support the monitoring of the Declaration on Digital Rights and Principles, available here: https://digital-strategy.ec.europa.eu/en/news-redirect/883230

further policy action under the Energy Efficiency Directive. The KPIs laid down 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 and insufficient information on the sustainability performance of data centres in the EU but it was also a significant step forward in putting in place the reporting and the respective platform. The second reporting cycle ends on 15 May 2025. Member States are encouraged to work with their respective national industries to improve their data collection, taking into account how critically important it is to have a good information basis for informing future policy choices. By 15 May 2025, the Commission will assess the available data and submit a report to the European Parliament and to the Council, exploring possible policy action such as minimum performance standards for new data centres.

The **Ecodesign for Sustainable Products Regulation** (**ESPR**), published in June 2024, aims to progressively set performance and information requirements for key products placed on the EU market, including ICT products. The Regulation introduces a '**Digital Product Passport'(DPP)**, which will be an easily accessible tag on products that will give prospective purchasers instant access to digital information about the product, including on product sustainability.

The ESPR authorises the Commission to adopt secondary legislation laying down the legal requirements for the DPP. This includes delegated and implementing acts concerning DPP service providers, digital credential procedures, central registry arrangements, and the lifecycle management of unique identifiers. Work on the delegated act aiming to set out the requirement for the future DPP service providers has already started. To this end, a public consultation and a study that will underpin the impact assessment are currently ongoing.

Another important work strand in the implementation process is the development of the DPP standards. The Commission plans to put forward a revision of the standardisation request to ensure the development of harmonised standards. The revised request will not touch upon the scope of the work set out in the original request. The standardisation efforts for the DPP extend beyond the EU's borders, with initiatives including UNECE's Recommendation no. 49 and collaborative projects involving international entities like ISO TC 154. The Commission follows closely these developments and works towards ensuring global interoperability and alignment.

The **CIRPASS project** ended in March 2024 and prepared the ground for the gradual piloting and deployment of the **Digital Product Passports (DPPs).** It is followed **by CIRPASS-2**, an innovation action project funded by the European Commission's Digital Europe Programme that started in May 2024 and will run until April 2027. This project builds on the results of CIRPASS and will demonstrate in 13 lighthouse pilots: (i) the functioning DPPs in real settings; and (ii) the benefits of these DPPs for the circular economy.

In June 2024, the EU adopted the **Directive on common rules promoting the repair of goods**. The Directive aims to promote the repair of goods within and beyond a product's legal guarantee. Within the legal guarantee, the consumers will be incentivised to opt for repair by extending the legal guarantee by one year for the repaired products. Beyond the legal guarantee, the Directive will oblige manufacturers to offer repair services for those products (including smartphones and tablets) that are subject to repairability requirements in EU law, under EU law on eco-design. The European Commission is mandated with establishing a European online repair platform to make it easier for consumers to find repair service providers.

The European Green Digital Coalition (EGDC) published in April 2024 a science-based method for estimating 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, which helped relevant organisations and experts to work with EGDC members to develop the Net Carbon Impact Assessment Methodology for ICT Solutions. For the first time, there is now a detailed and agreed methodology for calculating both the negative and positive carbon impact of digital solutions such as those used in a smart cities context. If the net impact of a digital solution is positive, then this gives the necessary evidence to policy makers and financial actors to support the scale up of such solutions.

In February 2025, the new EGDC Pilot 2 started. EGDC Pilot 2 will calculate 50 case studies from different sectors (including the smart cities sector) and bring financial institutions to develop eligibility criteria for climate (green) financing of the deployment of proven green digital (including AI) solutions.

Following up on the 2022 EU action plan on digitalising the energy system, the Commission published a study report in March 2024 on identifying common indicators for measuring the environmental footprint of electronic communications networks for the provision of electronic communications services. Building on this, the Commission is now working on drawing up an EU Code of Conduct for the sustainability of telecommunications networks by Q4 2025, in line with the action plan.

Member State action

Overall, 145 Member State initiatives related to the implementation of a sustainable digital transformation were identified by the support study, clearly indicating **the lowest level of activity in this area**. Efforts in this area mostly contribute to supporting the development and use of sustainable digital technologies that have minimal negative environmental and social impact (*24a)*, while only very few initiatives contribute to promoting sustainability standards and labels for digital products and services (*24d*).

Most initiatives are led by government organisations (77%), supported by actions originated by civil society, industry and National Human Rights Institutions. Initiatives are predominantly policy related (35%) or provide research and technological solutions in this area (28%). The vast majority of initiatives is put forward at national level (91%).

In 2024, some Member States were active in raising awareness about sustainable digitalisation, such as **Germany**. The Digital Sustainability Summit 2024 brought together industry, scientists and politicians to discuss and address issues of digital sustainability including green skills. **Malta**'s Digital Innovation Authority launched an applied research grant (MARG) to support capacity-building efforts related to: (i) technology for sustainability and environmental, social, and governance goals; and (ii) emerging technologies.

In **Italy**, the e-commerce consortium Netcomm is exploring how e-commerce and new retail can develop more sustainable supply chains and how digital technologies can help businesses tackle sustainability challenges, within its Digital Sustainability Working Group. Its 2025 work plan includes thematic meetings showcasing best practices and innovations in the sustainability of e-commerce and new retail.

Several other initiatives running over several years were ongoing in 2024. In **Latvia**, the Green Tech Cluster is a civil-society organisation that developed a cross-sectoral platform for companies, educational and research institutions, and other organisations operating in the green and smart technologies sectors. The cluster focuses on industries such as mechanical engineering, ICT, space technology, energy-efficient buildings, and environmentally-friendly raw materials. In **Austria**, the Green Tech Valley is a technology hotspot for climate protection and circular economy, housing 300 active green tech pioneers and technology leaders focused on green innovation.

Some Member States also put in place practical tools to help companies with their green transition. In **Denmark**, the Danish Business Authority runs the Climate Compass, which provides companies with a calculation of their greenhouse gas emissions and ideas on how to reduce their climate footprint.

The efforts of Member States in launching and running initiatives to promote digital sustainability rights may also be enabled by recent EU actions, including the Ecodesign for Sustainable Products Regulation and the Directive on Common Rules Promoting the Repair of Goods (both entered into force in 2024).

> **Best practice**
>
> In the **Netherlands**, the NGO Allemaal Digitaal celebrated three years of collecting, refurbishing and redistributing electronic devices to people without access to these devices themselves. With over 20 000 laptops, tablets and smartphones redistributed to date, the project has contributed to both reducing environmental waste and reducing inequality of opportunity by providing a digital device to people with low incomes. The recipients included older people, children, and people with a migrant background.