



# Study to support the monitoring of the Declaration on Digital Rights and Principles

Final Report

Written by Capgemini Invent, Visionary Analytics, IDC, Ecorys and Prof. Dr. Eleni Kosta (Independent Expert)  
May – 2025

DG CNECT

STUDY TO SUPPORT THE MONITORING OF THE DECLARATION ON  
DIGITAL RIGHTS AND PRINCIPLES

---

**EUROPEAN COMMISSION**

Directorate-General for Communications Networks, Content and Technology  
Directorate D — Policy Strategy and Outreach  
Unit D.2 — Policy Implementation and Planning

*Contact: Andrei Gaiu*

*E-mail: Andrei.GAIU@ec.europa.eu*

*European Commission  
B-1049 Brussels*

# **Study to support the monitoring of the Declaration on Digital Rights and Principles**

Final Report

Manuscript completed in May 2025

2<sup>nd</sup> edition

## LEGAL NOTICE

This document has been prepared for the European Commission however it reflects the views only of the authors, and the European Commission is not liable for any consequence stemming from the reuse of this publication. More information on the European Union is available on the Internet (<http://www.europa.eu>).

---

PDF ISBN 978-92-68-28064-5 doi: 10.2759/0915515 KK-01-25-083-EN-N

---

Luxembourg: Publications Office of the European Union, 2025

© European Union, 2025



The reuse policy of European Commission documents is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Except otherwise noted, the reuse of this document is authorised under a Creative Commons Attribution 4.0 International (CC-BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed provided appropriate credit is given and any changes are indicated.

For any use or reproduction of elements that are not owned by the European Union, permission may need to be sought directly from the respective rightholders.

## Abstract

The EU wants to promote and protect the digital rights of everyone living in the EU. The European Declaration on Digital Rights and Principles promotes a digital transition shaped by European values. The Declaration puts forward digital rights related principles and concrete commitments for the EU and Member States to act. This study supports the European Commission in monitoring the implementation and impact of this Declaration across the EU27 Member States. By using findings from desk research, statistical data, as well as a survey and workshop among stakeholders, it provides latest developments across the EU and the six Declaration Chapters. It also identifies key implementation and information gaps, as well as recommendations that could guide better implementation of digital rights and principles.

## Résumé

L'UE souhaite promouvoir et protéger les droits numériques de tous les citoyens de l'UE. La Déclaration européenne sur les droits et principes numériques encourage une transition numérique fondée sur les valeurs européennes. La Déclaration propose des principes liés aux droits numériques et des engagements concrets à prendre par l'UE et ses États membres. Cette étude soutient la Commission européenne à contrôler la mise en œuvre et l'impact de cette Déclaration dans les 27 États membres de l'UE. En utilisant les résultats de recherches documentaires, de données statistiques, ainsi qu'une enquête et un atelier parmi les parties prenantes, elle fournit les derniers développements à travers l'UE et les six chapitres de la Déclaration. Elle identifie également les principales lacunes en matière de mise en œuvre et d'information, ainsi que des recommandations qui visent à favoriser une meilleure application des droits et principes numériques.

## Executive Summary

The EU aims to promote and protect the digital rights and principles of everyone living in the EU. The European Declaration on Digital Rights and Principles for the Digital Decade (**the Declaration on Digital Rights and Principles**) stimulates governments and other stakeholders to respect these digital rights. In accordance with the Declaration, people need to be at the heart of the digital transformation and fully benefit from solidarity and inclusion in the digital environment. Everyone should have free and fair online choices, open participation in the digital public space, as well as safe, secure and empowered digital environments, while realising a sustainable digital future. The Declaration includes over 50 commitments for the EU and Member States to act in this respect, grouped in six main Chapters.

This study supports the European Commission in **monitoring the implementation and impact of the Declaration across the EU27 Member States**. It provides insights into the latest developments, identifies key implementation and information gaps, and offers recommendations for future action. Methodologically, the study combines desk research, statistical data, as well as a survey and workshop among stakeholders. Data collection covers government, civil society and industry stakeholders. Over 2,000 digital rights initiatives were identified across the EU27 Member States. These digital rights initiatives vary from legal initiatives, policy strategies, financial instruments, research and innovation projects, (technical) standards and guidelines, communication campaigns, training courses, digital rights observatories, etc.

The analysis of digital rights initiatives reveals that **most activity across EU27 Member States is associated with two main Declaration areas: *Solidarity and inclusion* (Chapter II) and *Safety, security and empowerment* (Chapter V)**, more specifically in the area of *Digital education, training and skills*, as well as *A protected, safe and secure digital environment*. Digital rights initiatives have also actively contributed to Commitments covered by *Putting people at the centre of the digital transformation* (Chapter I). Fewer digital rights initiatives were found for *Freedom of choice* (Chapter III), *Participation in the digital public space* (Chapter IV) and in particular *Sustainability* (Chapter VI).

**The total number of digital rights initiatives has been steadily growing over the years**, with new initiatives peaking in 2023. While fewer digital rights initiatives have been launched in 2024, the total number of ongoing initiatives is still increasing, with a majority of initiatives running for several years. Most of the digital rights initiatives are led by government organisations (over 80%), such as ministries, public agencies and municipalities. A more limited number of initiatives derive from (National) Human Rights Institutions, civil society and industry stakeholders. Furthermore, the vast majority of digital rights initiatives is being developed at the national level (close to 90%), while less activity is visible on the international, regional and local levels.

The study provides relevant quantitative data to the extent possible. Over 50 indicators shed light on the level of implementation of digital rights and principles on the ground, from the perspective of duty-bearers (mainly government, supported by civil society and industry stakeholders), and as perceived by rights-holders (e.g. citizens, consumers, employees and other persons living in the EU). For two thirds of the Declaration Commitments statistical sources can estimate their impact.

When looking at the quantitative impact indicators, **most impact and visible results in EU27 Member States are seen in the area of *Putting people at the centre of the digital transformation* (Chapter I) and *Solidarity and inclusion* (Chapter II)**, followed by *Freedom of choice* (Chapter III) and *Sustainability* (Chapter VI). On the other hand, initiatives in the area of *Participation in the digital public space* (Chapter IV) and *Safety, security and empowerment* (Chapter V) do not seem to show such protection of digital rights yet, regardless of Member States' efforts in the security and safety space relevant to the fifth Chapter. In general, duty-bearers such as governments tend to have more optimistic

stances towards the impact of digital rights initiatives than how they are perceived by rights-holders.

Some Declaration Commitments are rather broad and progress has so far proven to be more difficult to quantify, partly due to lack of available data. This challenge is visible across the various Declaration Chapters, but especially in the area of *Participation in the digital public space* (Chapter IV).

Based on these observations, the study recommends the EU27 Member States to **increase the Declaration's visibility and highlight the overall importance of digital rights and principles**. New initiatives are needed in areas merely overlooked at the moment, especially in the area of *Sustainability* (Chapter VI). In order for Member States to foster new initiatives in an effective and efficient way, existing initiatives could serve as a basis. Currently, most digital rights initiatives are led by government organisations. Wherever governments have paved the way, it is time for National Human Rights Institutions, civil society and industry stakeholders to build upon these initiatives and increase their efforts. In the spirit of the Declaration, such efforts may contribute most to the protection of people's digital rights whenever taken on by relevant stakeholders together. Similarly, most digital rights initiatives have a national scope. To maximise the Declaration's effects, nation-wide initiatives should be translated into international, regional and local initiatives and contexts too. Moreover, areas supported by relatively many digital rights initiatives should remain ongoing, such as *Solidarity and inclusion* (Chapter II) and *Safety, security and empowerment* (Chapter V).

Another set of recommendations invites the European Commission to coordinate efforts to improve the data availability for monitoring the progress in implementing digital rights and principles. The study outlines ways to **ensure a more comprehensive set of quantitative impact indicators**, for which annually collected data is available. This includes the exploration of new indicators with pilots in a selection of Member States and potentially scaling up digital rights measurements from the European Union Agency for Fundamental Rights, Council of Europe or United Nations. Indicators for *Participation in the digital public space* (Chapter IV) may be prioritised, as the measurement gaps are most apparent in this Chapter. The European Commission might also need to find replacing indicators for those deriving from the Berlin Declaration Monitoring Mechanism, which ended in 2024. Moreover, the Special Eurobarometer on the Digital Decade covers eleven Declaration Sub-chapters at the moment. By adding a survey item for the area of *Solidarity and inclusion* and *A fair digital environment* its coverage would increase. Both updates allow for maintaining a balance between the perspectives of duty-bearers (mainly based on the Berlin Declaration Monitoring Mechanism) and rights-holders (supported by the Special Eurobarometer on the Digital Decade). Data from annual measurements is preferred either way. Altogether, these efforts could ensure that the Declaration can be monitored effectively and continues to be relevant in the future.

## Synthèse

L'UE souhaite promouvoir et protéger les droits et principes numériques de tous les citoyens de l'UE. La Déclaration européenne sur les droits et principes numériques pour la Décennie numérique (**la Déclaration sur les droits et principes numériques**) incite les gouvernements et ses parties prenantes à respecter ces droits numériques. Conformément à la Déclaration, les citoyens doivent être au cœur de la transformation numérique et bénéficier pleinement de la solidarité et de l'inclusion dans l'environnement numérique. Chacun doit pouvoir faire des choix en ligne libres et justes, participer ouvertement à l'espace public numérique et bénéficier d'environnements numériques sûrs, sécurisés et autonomes, tout en réalisant un avenir numérique durable. La Déclaration comprend plus de 50 engagements pour l'UE et ses États membres, regroupés en six chapitres.

Cette étude soutient la Commission européenne à contrôler **la mise en œuvre et l'impact de la Déclaration dans les 27 États membres de l'UE**. Elle donne un aperçu des derniers développements, identifie les principales lacunes en matière de mise en œuvre et d'information, et propose des recommandations pour des actions futures. D'un point de vue méthodologique, l'étude combine des recherches documentaires, des données statistiques, ainsi qu'une enquête et un atelier réunissant les parties prenantes. La collecte de données couvre les parties prenantes des gouvernements, de la société civile et de l'industrie. Plus de 2 000 initiatives en matière de droits numériques ont été recensées dans les 27 États membres de l'UE. Ces initiatives de droits numériques sont diverses : initiatives juridiques, stratégies politiques, instruments financiers, projets de recherche et d'innovation, normes et directives (techniques), campagnes de communication, formations, observatoires des droits numériques, etc.

L'analyse des **initiatives en matière de droits numériques révèle que la plupart des activités dans les États membres de l'UE27 sont associées à deux domaines principaux de la Déclaration : *Solidarité et inclusion* (Chapitre II) et *Sûreté, sécurité et autonomisation* (Chapitre V)**, plus particulièrement dans le domaine de l'éducation, de la formation et des compétences numériques, ainsi qu'un environnement numérique protégé, sûr et sécurisé. Les initiatives en matière de droits numériques ont également contribué activement aux engagements couverts par l'initiative *Mettre les citoyens au cœur de la transformation numérique* (Chapitre I). Moins d'initiatives en matière de droits numériques ont été trouvées pour le *Libre-Arbitre* (Chapitre III), la *Participation à l'espace public numérique* (Chapitre IV) et en particulier de la *Durabilité* (Chapitre VI).

**Le nombre total d'initiatives en matière de droits numériques n'a cessé d'augmenter régulièrement au fil des années**, avec un pic de nouvelles initiatives en 2023. Alors que moins d'initiatives sur les droits numériques ont été lancées en 2024, le nombre total d'initiatives en cours continue d'augmenter, avec une majorité d'initiatives qui dure depuis plusieurs années. La plupart des initiatives en matière de droits numériques sont menées par des organisations gouvernementales (plus de 80 %), telles que des ministères, des agences publiques et des municipalités. Un nombre plus limité d'initiatives provient des institutions (nationales) des droits de l'homme, de la société civile et des parties prenantes de l'industrie. En outre, la grande majorité des initiatives en matière de droits numériques sont développées au niveau national (près de 90 %), qu'une activité plus limitée est visible au niveau international, régional et local.

L'étude fournit, dans la mesure du possible, des données quantitatives pertinentes. Plus de 50 indicateurs mettent en lumière le degré de mise en œuvre des droits et principes numériques sur le terrain, du point de vue des détenteurs d'obligation (principalement les gouvernements, soutenus par la société civile et les acteurs de l'industrie), et selon la perception des titulaires de droits (par exemple, les citoyens, les consommateurs, les employés et autres personnes vivant dans l'UE). Pour deux tiers des engagements de la Déclaration, des sources statistiques peuvent estimer leur impact.

Si l'on examine les indicateurs d'impact quantitatifs, c'est dans **les domaines *Mettre les citoyens au cœur de la transformation numérique* (Chapitre I) et la *Solidarité et***

**inclusion (Chapitre II)**, suivis de la *Liberté de choix (Chapitre III)* et de la *Durabilité (Chapitre VI)*, **que l'on observe le plus d'impact et de résultats visibles dans les États membres de l'UE27**. En revanche, les initiatives dans le domaine de la *Participation à l'espace public numérique (Chapitre IV)* et de la *Sûreté, sécurité et autonomisation (Chapitre V)* ne semblent pas encore montrer une telle protection des droits numériques quel que soient les efforts des États membres dans le domaine de la sécurité et de la sûreté relevant du cinquième chapitre. En général, les détenteurs d'obligations tels que les gouvernements ont tendance à être plus optimistes quant à l'impact des initiatives en matière de droits numériques que la façon dont elles sont perçues par les titulaires de droits.

Certains engagements de la Déclaration sont assez vastes et les progrès se sont avérés jusque-là plus difficiles à quantifier, en partie à cause du manque de données disponibles. Ce défi est visible dans les différents chapitres de la Déclaration, mais surtout dans le domaine de la *Participation à l'espace public numérique (Chapitre IV)*.

Sur la base de ces observations, l'étude recommande aux États membres de l'UE27 de **renforcer la visibilité de la Déclaration et de souligner l'importance générale des droits et principes numériques**. De nouvelles initiatives sont nécessaires dans des domaines actuellement négligés, en particulier dans le domaine de la *Durabilité (Chapitre VI)*. Pour que les États membres puissent favoriser de nouvelles initiatives de manière efficace et effective, les initiatives existantes pourraient servir de base. Actuellement, la plupart des initiatives en matière de droits numériques sont dirigées par des organisations gouvernementales. Là où les gouvernements ont ouvert la voie, il est temps que les institutions nationales des droits de l'homme, la société civile et les acteurs de l'industrie s'appuient sur ces initiatives et redoublent d'efforts. Dans l'esprit de la Déclaration, de tels efforts peuvent contribuer davantage aux droits numériques des personnes lorsqu'ils sont entrepris conjointement par les parties prenantes concernées. De même que, la plupart des initiatives en matière de droits numériques ont une portée nationale. Pour maximiser les effets de la Déclaration, les initiatives nationales devraient également être traduites en initiatives et contextes internationaux, régionaux et locaux. De plus, les domaines bénéficiant d'un certain nombre d'initiatives en matière de droits numériques devraient rester actifs, tels que *Solidarité et inclusion (Chapitre II)* et *Sûreté, sécurité et autonomisation (Chapitre V)*.

Une autre série de recommandations invite la Commission européenne à coordonner ses efforts pour améliorer la disponibilité des données permettant de suivre les progrès réalisés dans la mise en œuvre des droits et principes numériques. L'étude décrit des moyens de **garantir un éventail plus complet d'indicateurs d'impact quantitatif**, pour lesquels des données collectées annuellement sont disponibles. Il s'agit notamment d'explorer de nouveaux indicateurs à l'aide de projets pilotes dans une sélection d'États membres et d'étendre éventuellement, les mesures des droits numériques de l'Agence des droits fondamentaux de l'Union européenne (FRA), du Conseil de l'Europe ou des Nations Unies. Les indicateurs concernant la *Participation à l'espace public numérique (Chapitre IV)* pourraient être prioritaires, car c'est dans ce chapitre que les lacunes sont les plus évidentes en terme de quantification. La Commission européenne pourrait également avoir besoin de trouver des indicateurs de remplacement pour ceux issus du Mécanisme de suivi de la Déclaration de Berlin, qui a pris fin en 2024. De plus, l'Eurobaromètre spécial sur la Décennie numérique couvre actuellement onze sous-chapitres de la Déclaration. L'ajout d'un élément d'enquête dans le domaine de la Solidarité et de l'inclusion et d'un environnement numérique juste permettrait d'accroître sa diffusion. Les deux mises à jour permettent de maintenir un équilibre entre les perspectives des détenteurs d'obligations (principalement basées sur le Mécanisme de suivi de la Déclaration de Berlin) et des titulaires de droits (soutenus par l'Eurobaromètre spécial sur la Décennie numérique). Les données issues des relevés annuels sont préférés de toute façon. Ensemble, ces efforts permettrait d'assurer un suivi efficace de la Déclaration et de préserver sa pertinence à l'avenir.

## Glossary of Terms

- **The Declaration:** the Declaration on Digital Rights and Principles, officially known as "the European Declaration on Digital Rights and Principles for the Digital Decade", in short "the Declaration".
- **Declaration Chapter:** the Declaration has multiple layers and components. It consists of six main thematic Chapters:
  1. *Putting people at the centre of the digital transformation (Chapter I)*
  2. *Solidarity and inclusion (Chapter II)*
  3. *Freedom of choice (Chapter III)*
  4. *Participation in the digital public space (Chapter IV)*
  5. *Safety, security and empowerment (Chapter V)*
  6. *Sustainability (Chapter VI)*
- **Declaration Sub-chapter:** Declaration Chapters II, III and V are divided into 10 Sub-chapters. For Declaration Chapters I, IV and VI the Sub-chapters correspond with the 3 overall Chapter names:
  1. *Putting people at the centre of the digital transformation (Chapter I)*
  2. *Solidarity and inclusion (Chapter II)*
  3. *Connectivity (Chapter II)*
  4. *Digital education, training and skills (Chapter II)*
  5. *Fair and just working conditions (Chapter II)*
  6. *Digital public services online (Chapter II)*
  7. *Interactions with algorithms and artificial intelligence systems (Chapter III)*
  8. *A fair digital environment (Chapter III)*
  9. *Participation in the digital public space (Chapter IV)*
  10. *A protected, safe and secure digital environment (Chapter V)*
  11. *Privacy and individual control over data (Chapter V)*
  12. *Protection and empowerment of children and young people in the digital environment (Chapter V)*
  13. *Sustainability (Chapter VI)*
- **Declaration Principle:** the (Sub-)chapters come along 24 Principles. A Declaration Principle sets forth specific digital rights that are put into action through the Declaration Commitments.
- **Declaration Commitment:** the Declaration signatories agreed to live up to 51 concrete Commitments, across the Declaration (Sub-)chapters and Principles. With the Commitments, the signatories put the Declaration Principles into action.
- **Rights-holders:** persons holding the Declaration's digital rights and principles, those being affected by the implementation of digital rights by duty-bearers. All people in the EU may hold specific rights in their role as a citizen, consumer or for instance employee.
- **Duty-bearers:** organisations with responsibility to promote and protect the Declaration's digital rights and principles through implementation initiatives. Main duty-bearers are government bodies across the EU27 Member States, as well as EU institutions. In addition to the signatories of the Declaration, diligent action is expected from civil society and industry stakeholders.
- **Implementation initiative:** different types of activities and efforts from duty-bearers ranging from all sorts of legal instruments, policy instruments, financial instruments, research, innovation and collaboration instruments, communication instruments, harmonisation instruments, educational instruments, and monitoring instruments.

## Table of Contents

<b>1. Introduction – the Declaration on Digital Rights and Principles</b> .....	<b>14</b>
1.1. Promoting and protecting digital rights and principles.....	14
1.2. Monitoring the implementation of the Declaration.....	15
1.3. Reading Guide.....	15
<b>2. Methodological Approach – Combining Desk Research, Survey, Workshop and Statistical Data</b> .....	<b>16</b>
<b>3. Overall EU27 State of Play</b> .....	<b>18</b>
3.1. Implementation Initiatives .....	18
3.2. Impact Indicators and Visible Results .....	23
<b>4. Findings on Declaration Chapters</b> .....	<b>28</b>
4.1. Putting people at the centre of the digital transformation (Declaration Chapter I).....	29
4.1.1. Implementation Initiatives .....	29
4.1.2. Impact Indicators and Visible Results .....	32
4.2. Solidarity and inclusion (Declaration Chapter II).....	34
4.2.1. Implementation Initiatives .....	34
4.2.2. Impact Indicators and Visible Results .....	39
4.3. Freedom of choice (Declaration Chapter III).....	43
4.3.1. Implementation Initiatives .....	43
4.3.2. Impact Indicators and Visible Results .....	47
4.4. Participation in the digital public space (Declaration Chapter IV).....	49
4.4.1. Implementation Initiatives .....	49
4.4.2. Impact Indicators and Visible Results .....	53
4.5. Safety, security and empowerment (Declaration Chapter V) .....	54
4.5.1. Implementation Initiatives .....	54
4.5.2. Impact Indicators and Visible Results .....	59
4.6. Sustainability (Declaration Chapter VI).....	62
4.6.1. Implementation Initiatives .....	62
4.6.2. Impact Indicators and Visible Results .....	66
<b>5. Gaps and Challenges for Implementing and Measuring Declaration Progress</b> .....	<b>67</b>
5.1. Awareness and Communication .....	67
5.2. National Feedback and Reporting Channels .....	68
5.3. Future Priorities .....	68
5.4. Implementation and Data Gaps .....	69

<b>6. Conclusions and Recommendations .....</b>	<b>71</b>
<b>Annexes .....</b>	<b>73</b>
I. Country Factsheets.....	73
II. Data File (Excel) .....	73

# 1. Introduction – the Declaration on Digital Rights and Principles

## 1.1. Promoting and protecting digital rights and principles

The EU wants to promote and protect the digital rights of everyone living in the EU. The **Declaration on Digital Rights and Principles** is a foundational instrument in safeguarding shared European values in the digital era.<sup>1</sup> It is officially known as "the European Declaration on Digital Rights and Principles for the Digital Decade", in short "the Declaration".

As per the Declaration, people need to be at the heart of the digital transformation, embracing solidarity and inclusion. Everyone should have free and fair online choices, open participation in the digital public space, as well as safe, secure and empowered digital environments, while realising a sustainable digital future. Everyone should have an opportunity to shape the digital future. Altogether, the Declaration provides a **guiding set of rights and values** underlying the European Commission Digital Decade Targets and the Digital Decade Policy Programme 2030.<sup>2</sup> It ensures our digital economy and society reflect and respect the European spirit.

### European Declaration on Digital Rights and Principles for the Digital Decade

The European Parliament, the Council and the Commission solemnly proclaim the following joint Declaration on Digital Rights and Principles for the Digital Decade:

Preamble

We aim to provide a European way for the digital transformation, putting people at the centre, built on European values and EU fundamental rights, realising universal human rights, and benefiting all individuals, businesses, and societies as a whole.

We therefore declare:

**Chapter I: Putting people at the centre of the digital transformation**

1. People are at the centre of the digital transformation in the European Union. Technology should serve and benefit people living in the EU and empower them to pursue their aspirations, in full security and respect for their fundamental rights.

We commit to:

1. strengthening the democratic framework for a digital transformation that benefits everyone and improves the lives of all people living in the EU;
2. having human dignity at the centre of the EU and the rights of individuals at the heart of the digital transformation, as well as ensuring the full compliance with fundamental rights of the Declaration; such as having access to the public services online;
3. ensuring that the digital transformation, as well as ensuring the full compliance with fundamental rights such as data protection, the right to privacy, non-discrimination and gender equality, and with principles such as consumer protection, technological and non-technological transparency and explainability. It is also called for a strengthened protection of users' rights in the digital environment, as well as workers' rights and the right to disconnect<sup>3</sup>;
4. building on previous initiatives such as the "Digital Declaration on Governance" and the "Digital Declaration on Digital Security and Online Safety";
5. building on the "Digital Decade Policy Programme 2030" and the "Digital Declaration on Digital Security and Online Safety";
6. the EU will ensure that digital transformation is based on the common values and principles of the Declaration, such as having access to the public services online, as well as ensuring the full compliance with fundamental rights of the Declaration, such as data protection, the right to privacy, non-discrimination and gender equality, and with principles such as consumer protection, technological and non-technological transparency and explainability. It is also called for a strengthened protection of users' rights in the digital environment, as well as workers' rights and the right to disconnect<sup>3</sup>;

**Chapter II: Solidarity and inclusion**

1. Technology should be used to unite, and not divide, people. The digital transformation should contribute to a fair and inclusive society and economy in the EU.

We commit to:

1. making sure that the design, development, deployment and use of technological solutions respect fundamental rights, enable their access and promote solidarity and inclusion;
2. ensuring that digital transformation is based on the common values and principles of the Declaration, such as having access to the public services online, as well as ensuring the full compliance with fundamental rights of the Declaration, such as data protection, the right to privacy, non-discrimination and gender equality, and with principles such as consumer protection, technological and non-technological transparency and explainability. It is also called for a strengthened protection of users' rights in the digital environment, as well as workers' rights and the right to disconnect<sup>3</sup>;
3. developing adequate frameworks to that all make an action benefiting from the digital transformation in a fair and inclusive society and economy in the EU;

**Chapter III: Freedom of choice**

**Interventions with algorithms and artificial intelligence systems**

1. Artificial intelligence should serve as a tool for people, with the ultimate aim of increasing human well-being.

2. Everyone should be empowered to benefit from the advantages of algorithms and artificial intelligence systems without being subjected to undue surveillance or manipulation. Artificial intelligence should be used to support and enhance human decision-making, while being subjected to appropriate rules and to the law, safety and fundamental rights.

We commit to:

1. promoting human-centred, trustworthy and robust artificial intelligence systems throughout their development, deployment and use, in line with EU law;
2. ensuring an adequate level of transparency about the use of algorithms and artificial intelligence, and that people are empowered to use them and are informed when interacting with them;
3. ensuring that algorithms, systems are based on adequate datasets to avoid discrimination and enable better representation of all citizens, offering people safety and fundamental rights;
4. ensuring that technologies such as artificial intelligence are not used to prevent people's choice, for example targeting health, education, employment, and their private life;
5. providing for adequate and timely appropriate access, including by promoting trustworthy standards, to ensure that artificial intelligence and digital systems are, at all times, safe and used in full respect for fundamental rights;
6. taking measures to ensure that research in artificial intelligence respects the highest ethical standards and values in the EU;

**A fair digital environment**

1. Everyone should be able to effectively and freely choose which online services to use, based on objective, transparent, widely accessible and verifiable criteria.

2. Everyone should have the possibility to compare fairly and transparently in the digital environment. This should also benefit businesses and citizens.

We commit to:

1. ensuring access to high quality connectivity, with available internet access, for everyone wherever in the EU, including for those with low income;
2. protecting and promoting a stable and open internet where content, services, and applications are not unreasonably blocked or disrupted;
3. ensuring that digital education, training and lifelong learning and should also be equipping all users with necessary digital skills;
4. ensuring that digital education, training and lifelong learning and should also be equipping all users with necessary digital skills;

**Chapter IV: Participation in the digital public space**

1. Everyone should have access to a trustworthy, diverse and multidigital digital environment. Access should be guaranteed to a pluralistic public debate and effective participation in democracy in a non-discriminatory manner.

2. Everyone has the right to freedom of expression and information, as well as freedom of assembly and of association in the digital environment.

3. Everyone should be able to access information on who owns or controls the media services they are using.

4. Digital platforms, particularly very large online platforms, should support free democratic debate online. Cases of ill-use of platforms in the digital environment and business use of large online platforms should trigger the need for transparency and accountability of their services, including related to information and fundamental rights, and protect freedom of expression.

We commit to:

1. continuing safeguarding all fundamental rights, notably the freedom of expression and information, including media freedom and pluralism;
2. supporting the development and use of digital technologies to stimulate people's engagement and democratic participation;
3. supporting the development and use of digital technologies to stimulate people's engagement and democratic participation;
4. taking appropriate measures to tackle ill-use of digital content, in full respect for fundamental rights, including the right to freedom of expression and information, and without establishing any general monitoring obligation or censorship;
5. creating a digital environment where people are protected against discrimination and information manipulation and other forms of harmful content, including harassment and gender-based violence;
6. supporting effective access to digital content reflecting the cultural and linguistic diversity in the EU;
7. empowering individuals to make timely, given, specific choice and limiting the exploitation of vulnerabilities and biases, namely through targeted advertising;

**Chapter V: Safety, security and empowerment**

1. A protected, safe and secure digital environment.

2. Everyone should have access to digital technologies, products and services that are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided.

We commit to:

1. taking further measures to provide the availability of products and services that are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
2. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
3. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
4. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
5. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
6. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
7. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
8. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
9. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
10. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
11. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
12. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
13. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
14. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
15. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
16. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
17. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
18. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
19. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
20. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
21. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
22. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
23. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
24. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
25. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
26. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
27. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
28. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
29. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
30. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
31. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
32. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
33. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
34. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
35. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
36. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
37. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
38. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
39. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
40. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
41. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
42. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
43. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
44. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
45. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
46. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
47. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
48. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
49. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
50. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
51. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
52. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
53. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
54. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
55. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
56. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
57. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
58. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
59. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
60. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
61. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
62. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
63. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
64. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
65. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
66. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
67. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
68. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
69. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
70. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
71. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
72. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
73. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
74. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
75. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
76. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
77. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
78. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
79. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
80. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
81. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
82. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
83. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
84. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
85. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
86. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
87. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
88. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
89. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
90. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
91. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
92. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
93. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
94. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
95. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
96. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
97. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
98. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
99. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;
100. ensuring that digital technologies, products and services are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided;

**Chapter VI: Sustainability**

1. To avoid significant harm to the environment and to promote a circular economy, digital products and services should be designed, produced, used, repaired, recycled and disposed of in a way that mitigates their negative impact on the environment and on society and avoids premature obsolescence.

2. Everyone should have access to secure, trustworthy, and verifiable digital products and services, including digital products and services that are biologically secure, and privacy protective, meeting a high level of confidentiality, integrity, availability and authenticity of the information provided.

We commit to:

1. supporting the development and use of sustainable digital technologies that have minimal negative environmental and social impact;
2. recovering sustainably consumer choice and business models, and fostering sustainable and responsible corporate behaviour throughout global value chains of digital products and services, including a new to existing hardware;
3. promoting the development, deployment and active use of innovative digital technologies with a positive impact on the environment and society, and to accelerate the green transition;
4. promoting sustainability standards and labels for digital products and services;

For the European Parliament      For the Council of the European Union      For the European Commission

Roberto Meloni      Pto Filizos      Ursula von der Leyen  
The President      The President      The President

Figure 1. Signed version of the European Declaration on Digital Rights and Principles for the Digital Decade<sup>3</sup>

<sup>1</sup> <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles>

<sup>2</sup> [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en)

<sup>3</sup> <https://ec.europa.eu/newsroom/dae/redirection/document/94370>

The Declaration is not legally binding. Yet, it came into existence with the **highest political commitment**. The Declaration was signed on 15 December 2022 by the Presidents of the European Commission, European Parliament and Council of the European Union. The Declaration builds on the EU Charter of Fundamental Rights, Treaty on European Union, Treaty on the Functioning of the European Union and case-law of the Court of Justice of the European Union, as well as on secondary EU law.<sup>4</sup> It has been preceded by Declarations such as the Tallinn Declaration on eGovernment, Berlin Declaration on Digital Society and Value-Based Digital Government and Lisbon Declaration on Digital Democracy with a Purpose.<sup>5</sup>

## 1.2. Monitoring the implementation of the Declaration

The Declaration is closely linked to the **Digital Decade Policy Programme 2030**. The first and second annual State of the Digital Decade Reports were published in September 2023 and July 2024. These reports took stock of the EU's progress towards a successful digital transformation for citizens, businesses and the environment.<sup>6</sup> The monitoring of the Declaration on Digital Rights and Principles is an integral part of this annual State of the Digital Decade Report.

Monitoring the Declaration's implementation offers key insights into developments of promoting and protecting human rights in the digital era. To this end, the Commission prepared a Commission Staff Working Document on the Implementation of the Digital Decade objectives and the Digital Rights and Principles in 2023.<sup>7</sup> It was followed by a first Study to support the monitoring of the Declaration on Digital Rights and Principles, and the Commission's Monitoring of the European Declaration on Digital Rights and Principles (Annex 4 to the Second report on the State of the Digital Decade).<sup>8</sup> Against this background, the aim of this **Second study to support the monitoring of the Declaration on Digital Rights and Principles** is to provide systematic and consistent monitoring results, feeding into the 2025 edition of the State of the Digital Decade Report. It covers implementation initiatives by Member States, civil society and industry. It also analyses impact and provides recommendations on information and implementation gaps.

## 1.3. Reading Guide

The study report is structured as follows:

- Chapter 2: describes the **methodological approach**.
- Chapter 3: highlights the most important **EU findings** and trends.
- Chapter 4: presents the **Declaration Chapters' specific findings**.
- Chapter 5: sheds light on key **gaps and challenges** for the implementation of the Declaration and measuring progress.
- Chapter 6: provides the study's main **conclusions and recommendations**.
- Annexes: offer additional **background** data and information.

---

<sup>4</sup> [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC\\_2023\\_023\\_R\\_0001](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001)

<sup>5</sup> <https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration>, <https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government>, <https://futurium.ec.europa.eu/en/digital-compass/digital-principles/library-video/lisbon-declaration-digital-democracy-purpose>

<sup>6</sup> [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en)

<sup>7</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023SC0570>

<sup>8</sup> <https://digital-strategy.ec.europa.eu/en/library/monitoring-digital-rights-and-principles-support-study-2024>

## 2. Methodological Approach – Combining Desk Research, Survey, Workshop and Statistical Data

This study relies on **multiple methods** to collect data on the implementation of the Declaration. Findings are based on desk research, a survey and a stakeholder workshop as well as the analysis of statistical data sources that quantify the (perceived) impact of digital rights. The implementation and impact of the Declaration are measured on the level of the Declaration Chapters, Sub-chapters, Principles and Commitments, up and till the end of 2024.

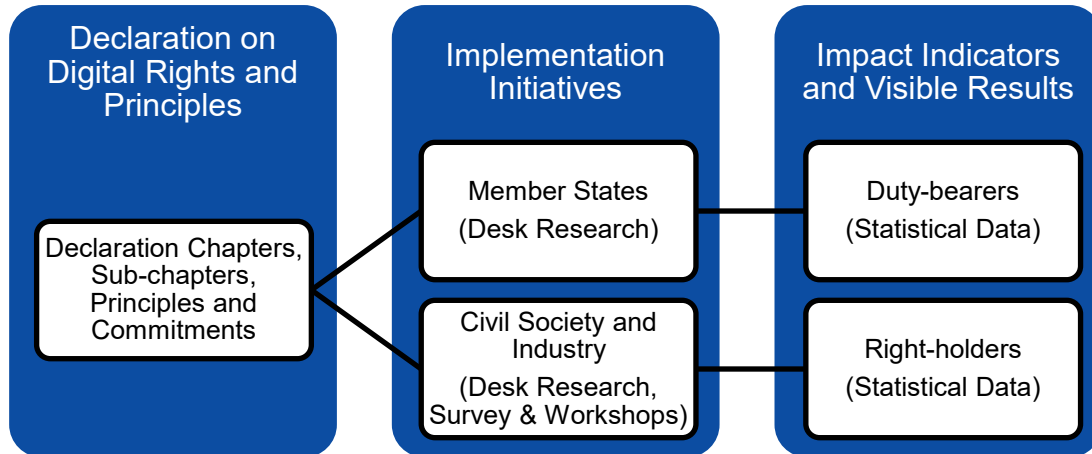


Figure 2. Overview of methodological approach

In order to identify **implementation initiatives** that strengthen the digital rights and principles laid down in the Declaration, extensive desk research has been conducted. Initiatives from government as well as civil society and industry stakeholders were included. Desk research was complemented with data from the Digital Decade Roadmap Measures Repository. Eleven Member States indicated which of their Digital Decade measures are linked to the implementation of the Declaration. These digital rights initiatives range from legal initiatives, policy strategies, financial instruments, research and innovation projects, (technical) standards and guidelines, communication campaigns, training courses, and digital rights observatories.

To bring on board additional views from civil society and industry, a public **stakeholder survey** was conducted. The online survey ran from 19 November 2024 until 24 January 2025. In total, 58 organisations from 16 Member States participated (representing 8 government organisations, 8 National Human Rights Institutions, 20 civil society actors, 12 businesses, 2 trade or labour unions, 2 consumer protection organisations and 6 representing other organisations, such as educational institutions). The stakeholder survey assessed awareness, implementation, and challenges related to the Declaration. It gathered insights on organisational engagement, existing feedback mechanisms, and strategies to enhance public awareness. Participants shared key digital rights initiatives, future priorities, and implementation barriers while providing recommendations to strengthen commitment and outreach efforts.

Moreover, on 23 January 2025, a **stakeholder workshop** was held, featuring three virtual breakout sessions. Close to 100 participants shared best practices and discussed future initiatives and actions related to specific Declaration Chapters. The workshop aimed to bring stakeholders together, present preliminary findings from the ongoing monitoring study, identify and address information gaps that could impede the implementation of digital rights initiatives, and facilitate knowledge-sharing among participants. It served as a complementary approach to the desk research, allowing stakeholders to contribute further insights to the monitoring study.

The Declaration's **impact and tangible results** have been analysed through (secondary) data sources, deriving from official EU statistical databases and previous studies. Impact shows the perspective of Member States as duty-bearers on the one hand. On the other hand, impact reflects how digital human rights-holders like citizens, consumers and employees perceive and experience the extent to which their digital rights are protected. An overview of all impact indicator data sources is provided in the Annex II.

To ensure highest reliability of findings, capture latest developments across the EU27 Member States and avoid potential misinterpretations, a **data review process** was put in place. National members of the Digital Decade Board were invited to review the final results for their Member State. For 26 of the 27 Member States, at least one national delegate reviewed the data underlying this Final Report.

### 3. Overall EU27 State of Play

A wide variety of government, civil society and industry stakeholders take action to promote and protect the digital rights of everyone living in the EU. What are overall implementation developments? How do various stakeholders bring to life the Declaration's digital rights and principles across the EU27 Member States?

#### 3.1. Implementation Initiatives

The study identified a total of **2,177 initiatives** across the EU27 Member States. Initiatives realise the digital rights and principles as outlined in the Declaration. Implementation initiatives come as different types of activities and efforts from duty-bearers. 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.

The analysis of the six **Declaration Chapters** in Figure 3 reveals that most initiatives are associated with *Solidarity and inclusion (Chapter II)* and *Safety, security and empowerment of individuals (Chapter V)*. It should be noted that these Declaration Chapters cover 8 of the 13 Sub-chapters and relatively many Commitments compared to the other Declaration Chapters, 29 of 51. Moreover, several targets from the Digital Decade Policy Programme are closely related to principles and commitments on *Solidarity and inclusion (Chapter II)*. Therefore, Member States are encouraged to act in these areas, such as improving basic digital skills and increasing the number of ICT specialists.<sup>9</sup> Next are initiatives focused on *Putting people at the centre of the digital transformation (Chapter I)* and *Freedom of choice (Chapter III)*. The areas of *Participation in the digital public space (Chapter IV)* and in particular *Sustainability (Chapter VI)* show least digital rights initiatives. Overall, 1711 (79%) initiatives address one of the Declaration Chapters, while 466 (21%) cover multiple Declaration Chapters. About one third of all initiatives, 949 (44%) cover a single Commitment, while 1228 (56%) initiatives support multiple Commitments. Further details on the coverage of specific Sub-chapters, Principles, and Commitments of the Declaration can be found in the dedicated sections below.

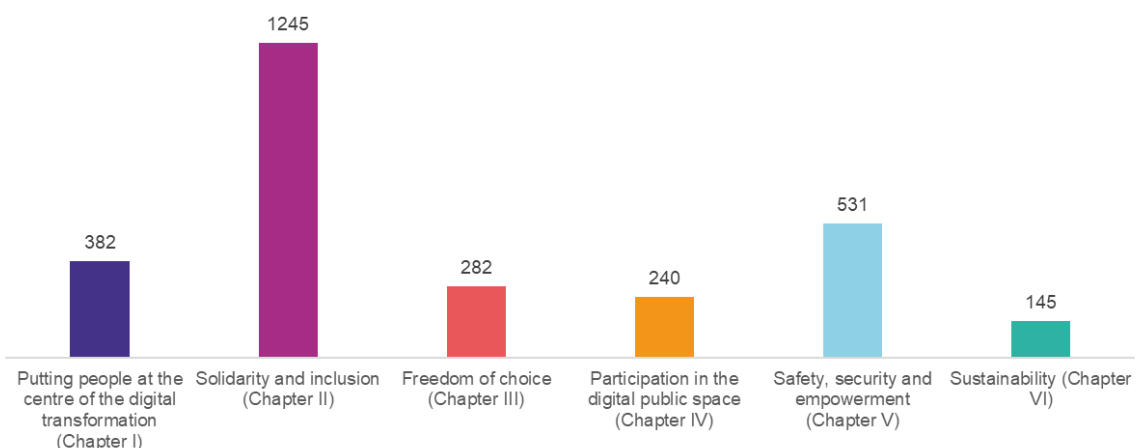


Figure 3. Number of implementation initiatives, per Declaration Chapter

Implementation initiatives were identified in all **EU27 Member States**. On average, 77 initiatives were found per country, aimed at strengthening digital rights and principles

<sup>9</sup> <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>

(Figure 4). Portugal, Luxembourg, Spain, Malta, Italy, Austria and Belgium have each launched over 100 digital rights initiatives, with Malta and Spain being the most active in launching new initiatives in 2024. The fewest digital rights initiatives were found in Slovakia, Latvia, Slovenia and Estonia. Although Greece, France, Lithuania and Slovakia have ongoing digital rights initiatives, no new initiatives were identified in 2024. In addition to the country-specific initiatives, 92 EU-wide initiatives were found. These policies and regulations apply to all EU27 Member States. It is important to note that the number of initiatives does not fully reflect the extent to which a digital right is protected and promoted. Some initiatives may include a wide range of sub-actions or run over several years, while other initiatives might be ad-hoc or target a more specific audience.

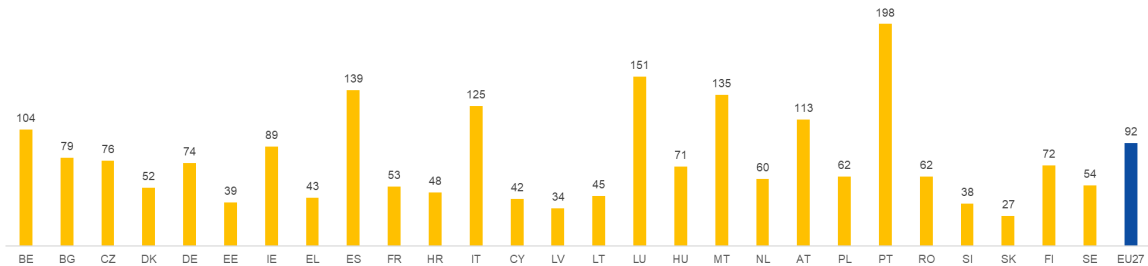


Figure 4. Number of implementation initiatives, per EU27 Member State

As shown in Figure 5, most of the digital rights initiatives are led by **government organisations**, such as ministries, public agencies and municipalities (1770 initiatives). A small number of initiatives come from (National) Human Rights Institutions (9), while a larger share is undertaken by civil society (266) and industry stakeholders (131). On one hand, governments are expected to be most active, as they are the main duty-bearers in digital rights. On the other hand, other stakeholders are ought to play a role too, knowing that some part of the Declaration Commitments directly target civil society and industry stakeholders to act, such as *Commitment 1c. fostering and ensuring responsible and diligent action by all actors, public and private, in the digital environment*, *Commitment 5-6b. ensuring that, in the working environment, digital tools do not put workers' physical and mental health at risk in any way*, and *Commitment 23-24d. promoting sustainability standards and labels for digital products and services*. Furthermore, it seems that thus far most (National) Human Rights Institutions have focused on other (long-standing) human rights Declarations, Treaties and Charters, in which digital rights are less at the forefront.

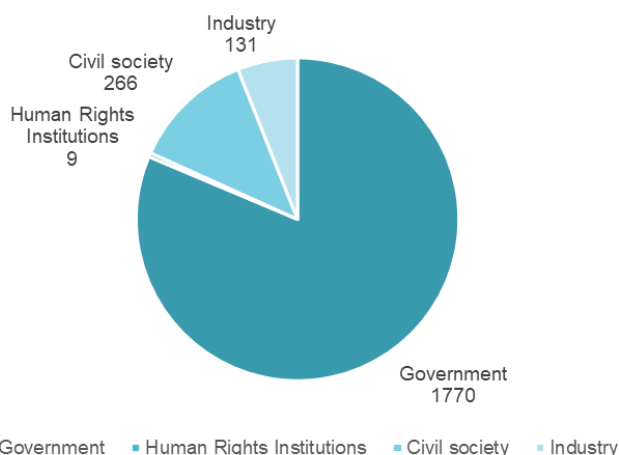


Figure 5. Number of implementation initiatives, per type of initiator

Digital rights initiatives vary in their **geographical scope** (Figure 6). Some are designed for specific parts of a country, while others address broad populations across entire countries. In reflecting the ambition to foster collaboration and cross-border efforts, 175 initiatives are international. This includes EU27 initiatives (EU initiatives with national transposition across

the EU27), EU MS initiatives (with two or more Member States working on a specific digital rights initiative) and EU MS+ initiatives (one or multiple EU Member States, working on a specific digital rights initiative with one or multiple non-EU countries).

At the country level, 1910 national initiatives span the entire Member State, reflecting a strong commitment to integrating EU-wide principles into domestic policies and aligning them with national priorities. Conversely, fewer initiatives were identified at the subnational level: provinces and regional authorities, city councils and local advocacy groups established 35 regional and 57 local digital rights initiatives. This disparity could suggest that while digital rights and principles are gaining traction at the national level, there is less activity or fewer resources dedicated to localised implementations. This reveals an opportunity for greater emphasis on regional and local activities, as visible to a certain extent in Belgium, Spain and Italy. This could help ensure digital rights and principles are accessible and responsive to the unique needs of smaller communities.



Figure 6. Number of implementation initiatives, per scope (international, national, regional and local)

Implementation initiatives can take various forms, as illustrated in Figure 7. The **type of initiative** may indicate how formal the efforts are. For instance, 255 initiatives are legal instruments, including laws, decrees, directives, legal acts, decisions, bills and legal proposals. The largest initiative category consists of 543 policy instruments, such as policy agendas and strategies, high-level implementation and action plans, or roadmaps. A smaller number of 146 financial instruments were found. Examples are investment programmes, subsidies, partnerships and joint actions. For research, innovation and collaboration instruments, the study identified 429 technological solutions, sectoral digital rights coalitions, pilots and experiments, regulatory sandboxes, etc. There are 108 harmonisation and standardisation instruments, aimed at standardising common practices, for instance by publishing concrete recommendations, guidelines, codes of conduct, (technical) standards, certification schemes, etc.

Compared to the previous initiatives, some actions are somewhat 'softer' and aim to stimulate digital rights and principles with communication instruments. This includes 234 communication and awareness raising campaigns. These initiatives are necessary, as people living in the EU often lack awareness of their digital rights, as explained in section 4.1 of this report, based on Special Eurobarometer on the Digital Decade findings. Similarly, educational tools help equip rights-holders with the right skills and competences. Member States have launched 391 training courses, educational measures, capacity-building activities. These initiatives are important, knowing that digital skills levels are a key challenge, as described in section 4.2 of the report. Lastly, some Member States seek to improve the digital rights and principles by implementing monitoring instruments. A total of 71 national monitoring and reporting initiatives, Key Performance Indicators (KPIs) and scoreboards were identified.

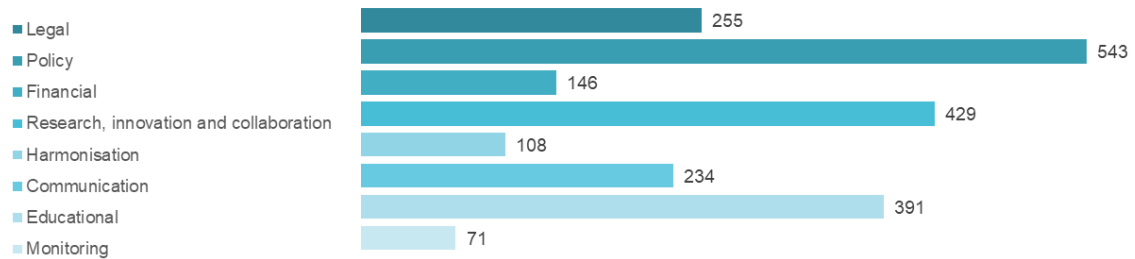


Figure 7. Types of implementation initiatives found, per type of initiative

From a **historical point of view**, Europe has a longstanding tradition of safeguarding fundamental rights. Some digital rights initiatives began before the Declaration was signed on 15 December 2022. Other initiatives started or were extended afterwards. For 1363 of the initiatives found in this study, the start year is known and shown in Figure 8. Besides initiatives from 2018 or earlier, the data shows a steady increase in new initiatives from 2019 to 2023.

*Solidarity and Inclusion (Chapter II)* consistently had the most activity, peaking in 2023 with 260 new initiatives, more precisely in the area of *Digital education, training and skills (Chapter II)*. As mentioned, priorities and efforts may be linked to the Digital Decade Policy Programme targets. *Putting people at the centre of the digital transformation (Chapter I)* also showed steady progress, with 108 new initiatives in 2023. In contrast, governments and other stakeholders launched only 21 new initiatives in 2024 for *Participation in the digital public space (Chapter IV)*, half the number compared to 2023. The area of *Sustainability (Chapter VI)* saw a similar pattern, with 32 new initiatives in 2023 and 15 in 2024. The only Declaration Chapter with more newly launched initiatives in 2024 than in 2023 is *Freedom of choice (Chapter III)*, with efforts intensified in the area of *Interactions with algorithms and artificial intelligence systems*. The EU AI Act which entered into force on 1 August 2024 could be a main driver for this trend.<sup>10</sup> Governments and other stakeholders started most of their *Safety, security and empowerment (Chapter V)* initiatives in 2018 or earlier, most likely due to the General Data Protection Regulation (GDPR) entering into force in 2018.<sup>11</sup>

The overall drop of new initiatives in 2024 brings the number back to 2022 levels. The 2023 peak could derive from the fact that the Declaration was just signed, but also by EU initiatives that reached political agreement or entered into force in the second half of 2022 and 2023 (such as the Cyber Resilience Act, Digital Markets Act, Digital Services Act).<sup>12</sup> Apart from these EU-driven developments, the number of new bottom-up initiatives from Member States seems to be stable since 2021. The fact that the number of new initiatives doubled between 2020 and 2021 may be explained by the Recovery and Resilience Facility (RRF), entered into force on 19 February 2021.<sup>13</sup> In light of the COVID-19 pandemic, the RRF funded recovery and resilience plans of the Member States until the end of 2026. Each Member State had to dedicate at least 20% of the budget to digital transition measures or actions to address challenges resulting from digitalisation. Another wave of new initiatives may occur in 2025. EU legislation such as the European Media Freedom Act and Ecodesign for Sustainable Products Regulation entered into force in 2024 and may spark new actions at national level in the coming time.

<sup>10</sup> <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

<sup>11</sup> [https://commission.europa.eu/law/law-topic/data-protection\\_en](https://commission.europa.eu/law/law-topic/data-protection_en)

<sup>12</sup> [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en)

<sup>13</sup> [https://commission.europa.eu/business-economy-euro/economic-recovery/recovery-and-resilience-facility\\_en](https://commission.europa.eu/business-economy-euro/economic-recovery/recovery-and-resilience-facility_en)

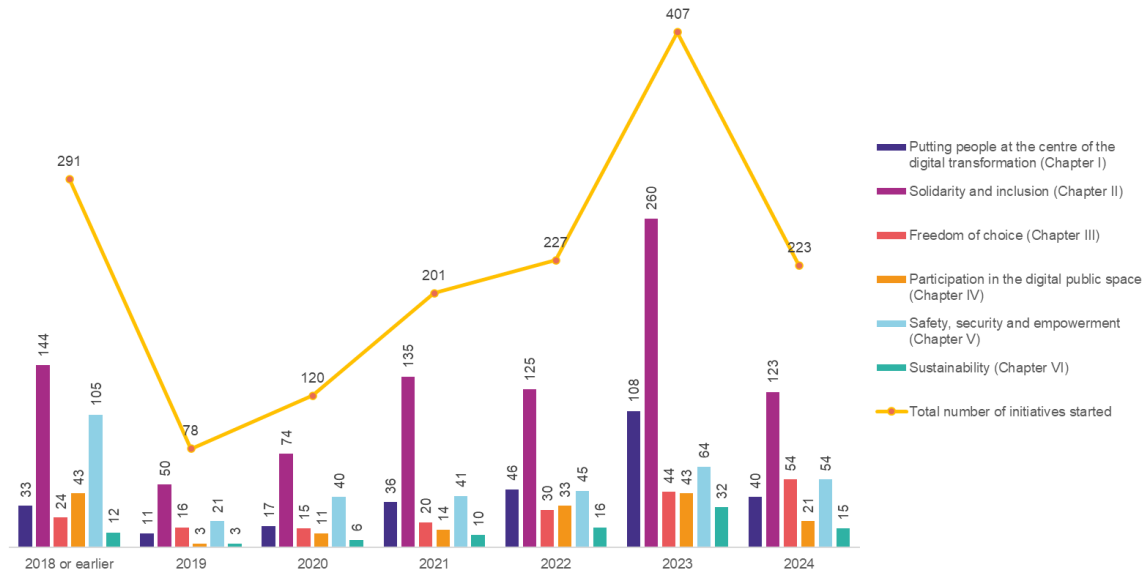


Figure 8. Number of implementation initiatives, per starting year and Declaration Chapter

It is worth mentioning that only 136 initiatives were active for one year. The other digital rights initiatives lasted two years or more, including ongoing policies and laws adopted for several years, as well as Digital Decade related initiatives and projects that last until 2030. In total, 86% of the identified digital rights initiatives are still ongoing. The cumulative picture shows that even though the number of new initiatives has been slowing down from 2024 onwards, the **total number of actively running digital rights initiatives** has still increased compared to previous years, i.e. doubled between 2021 and 2024.

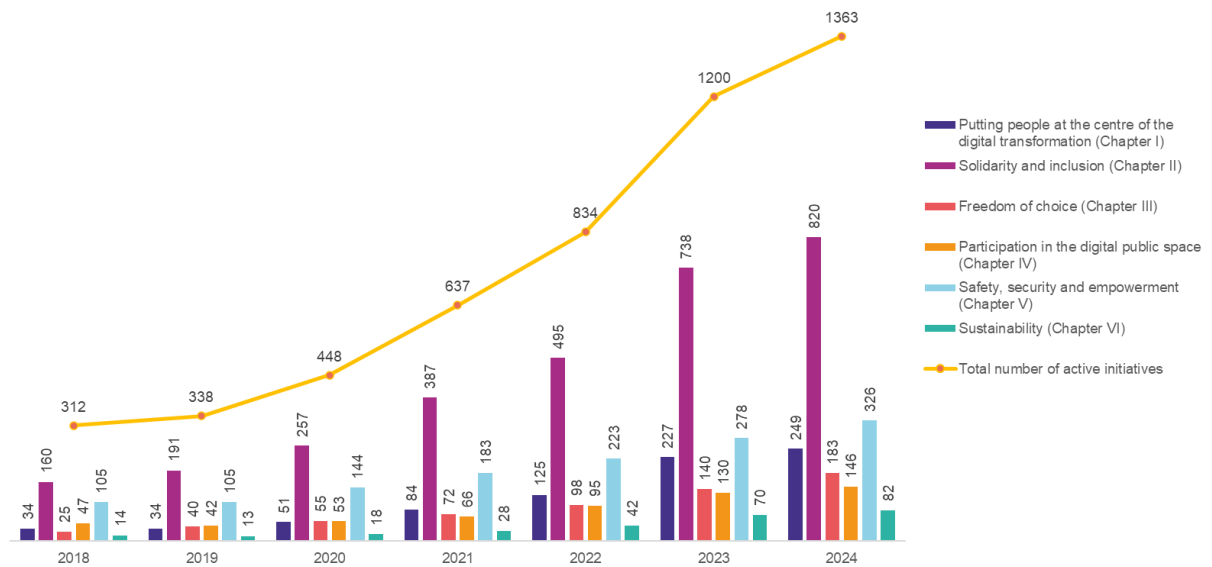


Figure 9. Number of implementation initiatives, ongoing, per year and Declaration Chapter

## 3.2. Impact Indicators and Visible Results

This study aims to map not only the digital rights initiatives that governments, civil society and industry implement, but also to analyse the **impact and visible results** stemming from these initiatives. To monitor the level of implementation of digital rights and principles across the EU27 Member States, a wide range of (quantitative) statistical sources has been taken into account. These indicators show to what extent duty-bearers are safeguarding specific Declaration (Sub-)chapters, Principles and Commitments and to what extent these are impacting the digital rights of rights-holders. In this context, duty-bearers are organisations with responsibility to promote and protect the Declaration's digital rights and principles through implementation initiatives. Main duty-bearers are government bodies across the EU27 Member States, as well as the three main EU institutions who are signatories of the Declaration. In addition to the signatories, diligent action is expected from civil society and industry stakeholders. Rights-holders are the persons holding the Declaration's digital rights and principles, those being affected by the implementation of digital rights by duty-bearers. All people in the EU may hold specific rights in their role as a citizen, consumer or for instance employee.

Given the broad scope of the Declaration, reliable and suitable **indicators** are available for some parts, whereas the impact of other Declaration areas is not yet measured, or not measured fully. For some Commitments, multiple statistical sources and indicators are available, whereas in other cases only a single source is used. When looking at the 51 Declaration Commitments, 34 can be supported with EU27 data on impact, collected in 2020 or more recent. This consists of 26 duty-bearer related indicators (e.g. government statistics on established connectivity or eHealth services) and 25 rights-holder related indicators (e.g. citizen views shared through the Special Eurobarometer on the Digital Decade). For the remaining 17 Declaration Commitments, no relevant indicator data is currently available. A full overview of all indicators and data sources per Declaration Commitment can be found in the Data File (Excel) attached to this report.

	Commitments with EU27 data	Commitments without EU27 data
<b>Chapter I.</b>	3/4 Commitments with EU27 data 1 duty-bearers related indicators 2 rights-holders related indicators	1/4 Commitments without EU27 data
<b>Chapter II.</b>	12/17 Commitments with EU27 data 14 duty-bearers related indicators 10 rights-holders related indicators	5/17 Commitments without EU27 data
Solidarity and inclusion	2/3 <i>Commitments with EU27 data</i> 3 <i>duty-bearers related indicators</i> 1 <i>rights-holders related indicators</i>	1/3 <i>Commitments without EU27 data</i>
Connectivity	1/2 <i>Commitments with EU27 data</i> 1 <i>duty-bearers related indicators</i> 1 <i>rights-holders related indicators</i>	1/2 <i>Commitments without EU27 data</i>
Digital education, training and skills	4/4 <i>Commitments with EU27 data</i> 3 <i>duty-bearers related indicators</i> 4 <i>rights-holders related indicators</i>	0/4 <i>Commitments without EU27 data</i>

<i>Fair and just working conditions</i>	2/5 Commitments with EU27 data 2 duty-bearers related indicators 2 rights-holders related indicators	3/5 Commitments without EU27 data
<i>Digital public services online</i>	3/3 Commitments with EU27 data 4 duty-bearers related indicators 1 rights-holders related indicators	0/3 Commitments without EU27 data
<b>Chapter III.</b>	5/8 Commitments with EU27 data 4 duty-bearers related indicators 1 rights-holders related indicators	3/8 Commitments without EU27 data
<i>Interactions with algorithms and artificial intelligence systems</i>	4/6 Commitments with EU27 data 3 duty-bearers related indicators 1 rights-holders related indicators	2/6 Commitments without EU27 data
<i>A fair digital environment</i>	1/2 Commitments with EU27 data 1 duty-bearers related indicators 0 rights-holders related indicators	1/2 Commitments without EU27 data
<b>Chapter IV.</b>	3/6 Commitments with EU27 data 1 duty-bearers related indicators 2 rights-holders related indicators	3/6 Commitments without EU27 data
<b>Chapter V</b>	7/12 Commitments with EU27 data 2 duty-bearers related indicators 8 rights-holders related indicators	5/12 Commitments without EU27 data
<i>A protected, safe and secure digital environment</i>	2/3 Commitments with EU27 data 1 duty-bearers related indicators 2 rights-holders related indicators	1/3 Commitments without EU27 data
<i>Privacy and individual control over data</i>	3/4 Commitments with EU27 data 1 duty-bearers related indicators 4 rights-holders related indicators	1/4 Commitments without EU27 data
<i>Protection and empowerment of children and young people in the digital environment</i>	2/5 Commitments with EU27 data 0 duty-bearers related indicators 2 rights-holders related indicators	3/5 Commitments without EU27 data
<b>Chapter VI.</b>	4/4 Commitments with EU27 data 4 duty-bearers related indicators 2 rights-holders related indicators	0/4 Commitments without EU27 data

Table 1. Data availability impact indicators for EU27

The quantitative impact indicators as mentioned above provide a view on the extent to which digital rights and principles are respected in the EU27. How well are the principles and

commitments in the six Declaration Chapters put into practice? In order to answer this question the indicator values for each of the Declaration Chapters were aggregated to compute EU27 averages. **Average Declaration Chapter scores** were calculated for all indicators with 2023 data, since most indicators had data available for that year (42, compared to 20 indicators with 2024 numbers). The 42 indicators that contain 2023 data consist of 21 indicators related to duty-bearers and the other 21 indicators related to rights-holders.

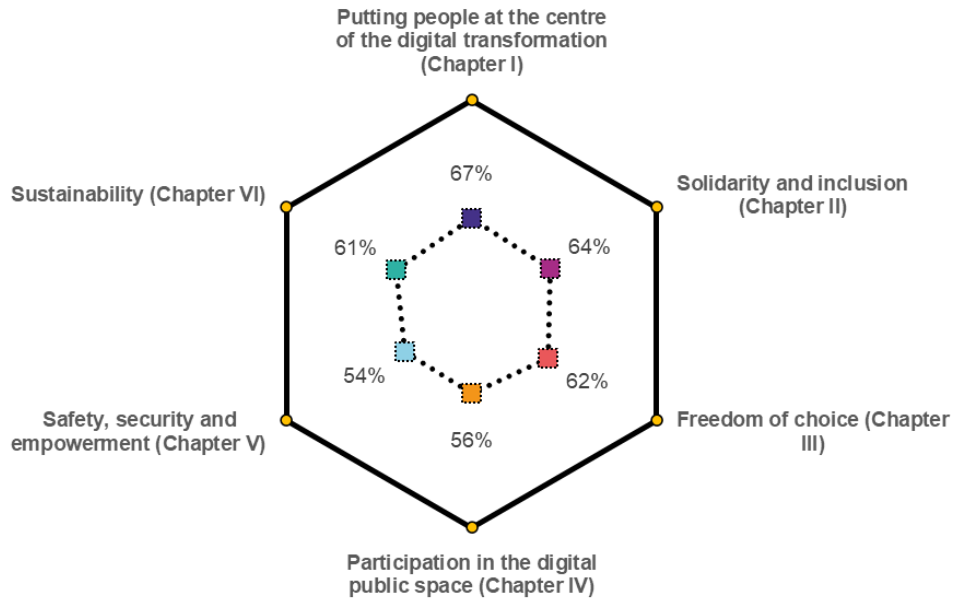


Figure 10. Indicative aggregate values for the impact indicators in 2023, per Declaration Chapter

When overseeing all six Declaration Chapters and taking into account the impact levels of the underlying Declaration Commitments (Figure 10), it seems that **the areas of *Putting people at the centre of the digital transformation (Chapter I)* and *Solidarity and inclusion (Chapter II)* bring about most impact at the moment**. These Declaration Chapters observe relative high impact from duty-bearers and rights-holders feel their rights are highly respected too, foremost in countries like Finland, Luxembourg and Malta. On the basis of available statistics it seems that the digital rights and principles in *Participation in the digital public space (Chapter IV)* and *Safety, security and empowerment (Chapter V)* are respected least so far. Indicators that reflect the impact from duty-bearers, as well as indicators that show rights-holders' views are at a relatively low level for these two Declaration Chapters.

It is important to note that even though the quantitative indicators can provide insights into implementation developments, percentages from 0%-100% cannot fully capture the contextual complexity of digital rights and cannot indicate a digital right to be 'completed' whenever an indicator is reaching a high level in relation to other indicators. Furthermore, the indicative aggregates do not take into account the Declaration Commitments for which no reliable data is available at the moment. This may bias the actual extent to which duty-bearers respect the digital rights of rights-holders and how rights-holders experience their digital rights.

In general, the **duty-bearer related impact indicators show higher impact levels than those related to the views of rights-holders**. In other words, duty-bearers such as governments present more optimistic findings than looking at the views from citizens, consumers, employees and other rights-holders living in the EU. For 2023, the average digital rights impact level sits at 70% based on duty-bearers related indicators versus 53% for rights-holders. This may indicate that duty-bearers are too optimistic about the effects of their actions in some digital rights areas on the one hand, whereas rights-holders may not be fully aware of the extent to which their digital rights are protected and promoted. The gap

between duty-bearers and rights-holders might not be bridged soon. The 2025 Special Eurobarometer on the Digital Decade shows that citizen perceptions are rather unchanged compared to 2024 and 2023.<sup>14</sup> For most of the 17 digital rights and principles that were surveyed, just half of the EU population believes these are sufficiently protected. As described in the next chapter, no or limited progress has been made with mainly only 1 or 2 percentage points increases or decreases.

**The divide between duty-bearers and rights-holders is most visible in the area of *Putting people at the centre of the digital transformation (Chapter I)***, although the available indicators are hard to compare. In fact, the duty-bearer related indicator covers *Commitment 1c. fostering and ensuring responsible and diligent action by all actors, public and private, in the digital environment*, while the rights-holders perceptions relate to *Commitment 1a. strengthening the democratic framework for a digital transformation that benefits everyone and improves the lives of all people living in the EU*, and *Commitment 1b. taking necessary measures to ensure that the values of the EU and the rights of individuals as recognised by EU law are respected online as well as offline*. The only area where duty-bearers are less optimistic than rights-holders is *Solidarity and inclusion (Chapter II)*. Again, indicators do not mirror. The internet usage among marginalised groups (rights-holders perceptive) cannot be compared directly with the web accessibility levels as established by government (duty-bearers perspective), even though both are related to *Commitment 2b. a digital transformation that leaves nobody behind. It should benefit everyone, achieve gender balance, and include notably elderly people, people living in rural areas, persons with disabilities, or marginalised, vulnerable or disenfranchised people and those who act on their behalf. It should also promote cultural and linguistic diversity*. All impact numbers are listed in the table below and all related indicators are presented in section 4 of this report:

	Duty-bearers indicators (2023)	Rights-holders indicators (2023)
<b>Chapter I.</b>	1 duty-bearers related indicators 90%	2 rights-holders related indicators 60%, 52%
<b>Chapter II.</b>	12 duty-bearers related indicators	8 rights-holders related indicators
<i>Solidarity and inclusion</i>	3 duty-bearers related indicators 74%, 45%, 35%	1 rights-holders related indicators 90%
<i>Connectivity</i>	1 duty-bearers related indicators 63%	1 rights-holders related indicators 53%
<i>Digital education, training and skills</i>	3 duty-bearers related indicators 71%, 53%, 87%	3 rights-holders related indicators 54%, 56%, 24%
<i>Fair and just working conditions</i>	1 duty-bearers related indicators 87%	2 rights-holders related indicators 51%, 60%
<i>Digital public services online</i>	4 duty-bearers related indicators 92%, 76%, 98%, 76%	1 rights-holders related indicators 54%
<b>Chapter III.</b>	4 duty-bearers related indicators	1 rights-holders related indicators

<sup>14</sup> Special Eurobarometer 532, 551 and 103.2 on the Digital Decade, <https://europa.eu/eurobarometer/surveys/detail/3174>

<i>Interactions with algorithms and artificial intelligence systems</i>	3 duty-bearers related indicators 61%, 64%, 74%	1 rights-holders related indicators 49%
<i>A fair digital environment</i>	1 duty-bearers related indicators 62%	0 rights-holders related indicators -
<b>Chapter IV.</b>	0 duty-bearers related indicators -	2 rights-holders related indicators 60%, 52%
<b>Chapter V</b>	1 duty-bearers related indicators	6 rights-holders related indicators
<i>A protected, safe and secure digital environment</i>	0 duty-bearers related indicators -	1 rights-holders related indicators 55%
<i>Privacy and individual control over data</i>	1 duty-bearers related indicators 72%	3 rights-holders related indicators 49%, 51%, 40%
<i>Protection and empowerment of children and young people in the digital environment</i>	0 duty-bearers related indicators -	2 rights-holders related indicators 66%, 45%
<b>Chapter VI.</b>	4 duty-bearers related indicators 74%, 59%, 64%, 72%	2 rights-holders related indicators 48%, 51%

Table 2. Duty-bearers and rights-holders related impact indicators, EU27 averages for 2023

## 4. Findings on Declaration Chapters

This section provides a closer look into the **six Declaration Chapters**. Each Declaration Chapter analysis begins with a fictive persona story to exemplify how digital rights and principles can make a difference in the personal lives of all persons living in the EU. Both the implementation initiatives within each Chapter and the impact are analysed. Furthermore, quotes from the stakeholder survey and collected good practices are included to enrich the Declaration Chapter specific insights.

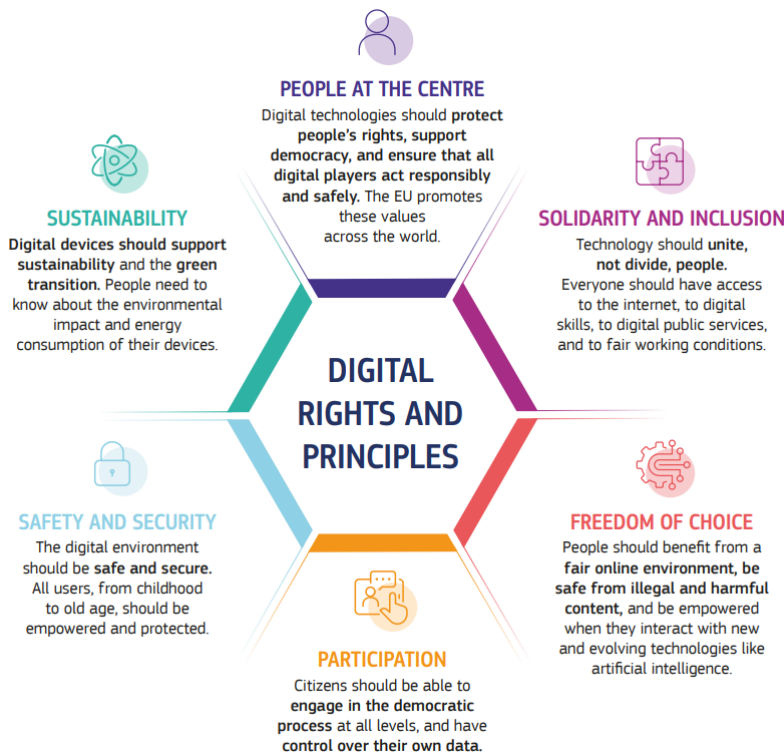


Figure 11. The six Chapters of the European Declaration on Digital Rights and Principles for the Digital Decade

## 4.1. Putting people at the centre of the digital transformation (Declaration Chapter I)

At the heart of the EU's commitment to a fair digital future is a core principle: putting people at the centre of the digital transformation. This means not only ensuring that technology supports individuals and protects their rights but also that it works for everyone, regardless of their background. As for the other Declaration Chapter analyses, this section begins with a fictive persona story. It illustrates how digital rights can make a difference in the personal lives of all persons living in the EU. Regardless of them holding EU citizenship. The story below reflects what this vision could look like in practice, as the personas navigate the digital landscape, striving to ensure that people's rights remain a priority.

### *Ana-Sofia and Gabriel*

*Ana-Sofia and Gabriel are a couple living and working in the EU. Anna-Sofia is a local citizen, while Gabriel received his EU-citizenship after finishing his law degree and moving to Europe. Both are lawyers active within their community and have been impressed how the EU values are culturally rooted. Luckily, their government does not take this for granted. Ministries and decentral authorities continue to strengthen the democratic framework for a digital transformation that improves the lives of all people living in the EU. And it's not just the government who takes action. In their city, next to the watercourse of the Danube, they notice diligent action by a wide variety of actors in the digital environment. Both public and private, including their law firm. Hence, they feel their rights are respected equally offline as online. Their country also actively shares the EU view on putting people at the centre of the digital transformation on the international stage. They proudly heard the news that their country now collaborates on digital rights with Gabriel's country of birth too.*

Ana-Sofia and Gabriel's experience reflects the broader challenge within the EU's digital transformation. While technology has the potential to improve access to services, it must be inclusive and consider the diverse needs of all residents, regardless of their citizenship status. The EU's commitment to putting people at the centre of digital transformation must extend beyond technological innovation, ensuring that digital systems serve everyone equally and protect the rights of all citizens in an increasingly digital world.

### 4.1.1. Implementation Initiatives

Across the EU27 Member States, 382 initiatives can be linked to *Putting people at the centre of the digital transformation* (Chapter I). In particular the following Sub-chapters, Principles and Commitments are covered by the implementation efforts:

Putting people at the centre of the digital transformation (Chapter I)	382
<i>Principle 1. People are at the centre of the digital transformation in the European Union. Technology should serve and benefit all people living in the EU and empower them to pursue their aspirations, in full security and respect for their fundamental rights.</i>	381
Commitment 1a. strengthening the democratic framework for a digital transformation that benefits everyone and improves the lives of all people living in the EU	280

Commitment 1b. taking necessary measures to ensure that the values of the EU and the rights of individuals as recognised by EU law are respected online as well as offline	204
Commitment 1c. fostering and ensuring responsible and diligent action by all actors, public and private, in the digital environment	191
Commitment 1d. actively promoting this vision of the digital transformation, also in our international relations	182

Table 3. Number of initiatives related to Putting people at the centre of the digital transformation (Chapter I)

From the initiatives with a link to **Putting people at the centre of the digital transformation (Chapter I)**, the highest number of initiatives focus on *Commitment 1a. strengthening the democratic framework for a digital transformation that benefits everyone and improves the lives of all people living in the EU*. The number of initiatives that take action on the other Commitments is relatively similar. Most initiatives are led by government organisations (320, compared to 42 civil society, 16 industry initiatives and 4 from National Human Rights Institutions). Initiatives are predominantly policy related (118) or research and technology projects (85). With 327 initiatives at the national level, digital rights and principles in this field are mostly promoted and protected nationally. In addition, 21 initiatives are taken on by the EU27 collectively, 6 initiatives are performed by a smaller group of EU Member States. On the regional level 4 initiatives have been ongoing, whereas 8 local initiatives were found. From a historical point of view, most initiatives started in 2023, with 108 initiatives launches.

### Spain Good Practice – Observatorio de Derechos Digitales (*Digital Rights Observatory*)

- **Objectives:** The Digital Rights Observatory (2025 – Ongoing) in Spain, announced by President Pedro Sánchez, aims to promote and defend citizens' rights in the digital world, aligning with Spain's Charter of Digital Rights, from 2021.
- **Description:** As a public-private initiative led by Red.es and mainly funded by NextGeneration EU, the Observatory works to implement digital rights across various sectors, ensuring privacy, security, and equality online. The Observatory is supported by more than 150 entities and 350 experts, including experts in the field of digital rights and technology, representatives of public institutions and civil society organisations. This wide representation fosters and ensures responsible and diligent action by all actors in the digital environment, public and private.
- **Stakeholder benefits:** The Observatory aims to provide an open, inclusive and participatory space, to inform citizens about the progress, advantages and challenges in the field of digital rights and to promote good practices. Citizens benefit from stronger protections in digital environments, businesses gain clearer guidelines for digital operations, and public institutions enhance their ability to enforce rights in emerging tech spaces.
- **Accelerating mechanisms:** The Observatory's efforts are backed by agreements with public and private stakeholders and a €10.83 million budget from EU recovery funds. It focuses on key areas, including cybersecurity, equality, workplace rights, and new technologies like AI and the metaverse.
- **Link for more information:** <https://www.derechosdigitales.gob.es/en>



#### PEOPLE AT THE CENTRE

Digital technologies should protect people's rights, support democracy, and ensure that all digital players act responsibly and safely. The EU promotes these values across the world.

## Belgium Good Practice – DigitAll

- **Objectives:** To enhance digital inclusion in Belgium by providing access to digital tools and skills for all citizens (2020 – Ongoing).
- **Description:** Runs awareness campaigns showing how digital exclusion affects fundamental rights like health, education, and work.
- **Stakeholder benefits:** Organisations benefit from shared resources and a stronger commitment to social responsibility. Citizens gain better access to digital tools, improving their participation in society and the workforce.
- **Accelerating mechanisms:** Collaboration, awareness campaigns, and resource sharing help drive the success of DigitAll's initiatives.
- **Link for more information:** <https://digitall.be/who-are-we>



### PEOPLE AT THE CENTRE

Digital technologies should **protect** people's rights, support democracy, and ensure that all digital players act responsibly and safely. The EU promotes these values across the world.

## Finland Good Practice - Tampere Metaverse Vision 2040

- **Objectives:** To leverage advanced technologies to enhance citizens' well-being, urban governance, sustainability, equality, and healthcare by integrating the metaverse into city development (2023 – Ongoing).
- **Description:** Explores how a metaverse environment, comprising various intelligent technologies, can support key priorities such as citizen happiness, effective governance, environmental sustainability, social equality, and improved healthcare services.
- **Stakeholder benefits:** City planners and administrators can use digital twins and AI-driven tools to simulate urban scenarios, leading to more informed decision-making and efficient resource management. Residents benefit from personalised services in education, well-being, and urban living, while businesses and tourists can engage with the city virtually, enhancing economic growth and social integration.
- **Accelerating mechanisms:** Strong public-private collaboration, government support and funding, focus on citizen well-being, advanced technology integration, sustainability and inclusivity
- **Link for more information:** <https://metaverse-institute.org/tampere-metaverse-vision-2040-unveils-the-potential-of-a-future-city-leveraging-advanced-technologies/>



### PEOPLE AT THE CENTRE

Digital technologies should **protect** people's rights, support democracy, and ensure that all digital players act responsibly and safely. The EU promotes these values across the world.

### Bulgaria Good Practice – Rights in the Loop

- **Objectives:** To promote human rights compliance in the digital space by engaging stakeholders and raising awareness (2023 – Completed).
- **Description:** The project involves building a network of supportive journalists to share success stories about technology and human rights compliance.
- **Stakeholder benefits:** Enhanced collaboration and resource sharing among organisations focused on human rights. Increased public awareness of human rights issues in the digital environment.
- **Accelerating mechanisms:** Effective communication strategies and partnerships with media outlets to disseminate information.
- **Link for more information:** <https://bcnl.org/en/projects/rights-in-the-loop-spotlighting-human-rights-in-the-digital-space>



#### PEOPLE AT THE CENTRE

Digital technologies should protect people's rights, support democracy, and ensure that all digital players act responsibly and safely. The EU promotes these values across the world.

### Luxembourg Good Practice – Luxinnovation

- **Objectives:** To foster innovation, support economic development, and enhance the competitiveness of Luxembourg's economy by assisting companies and public research institutions (1984 – Ongoing).
- **Description:** Serves as Luxembourg's national innovation agency, offering services such as funding guidance, startup support, and performance improvement programs to drive innovation across various sectors. By advising companies on technologies such as Artificial Intelligence, Cybersecurity and eHealth and their impact on users, Luxinnovation promotes responsible and diligent action by all actors in the digital environment including businesses.
- **Stakeholder benefits:** Government bodies and research institutions benefit from strengthened collaboration and alignment with national economic objectives. Companies receive support in innovation, funding, and market insights, enhancing their competitiveness and growth potential.
- **Accelerating mechanisms:** Initiatives like "Fit 4 Start" provide startups with coaching, funding, and resources, accelerating their development. Strong network and collaboration, market insight and guidance.
- **Link for more information:** <https://www.luxinnovation.lu/>



#### PEOPLE AT THE CENTRE

Digital technologies should protect people's rights, support democracy, and ensure that all digital players act responsibly and safely. The EU promotes these values across the world.

## 4.1.2. Impact Indicators and Visible Results

When it comes to *Commitment 1a. strengthening the democratic framework for a digital transformation that benefits everyone and improves the lives of all people living in the EU*, impact indicators point out the importance of ongoing efforts and need to strengthen digital rights holistically. The Special Eurobarometers 532, 551 and 103.2 on the Digital Decade, show that in 2025 just 44% of EU rights-holders think that the EU protects their rights in the

digital environment well. This has been declining from 45% in 2024 and 50% in 2023.<sup>15</sup> It seems that a majority of citizens is worried about their digital rights. It appears that citizens feel that their government and the EU are insufficiently able to protect them from threats in the digital environment and more action is needed.

In terms of *Commitment 1b. taking necessary measures to ensure that the values of the EU and the rights of individuals as recognised by EU law are respected online as well as offline*, a similar picture is visible. Many rights, such as freedom of expression, the protection of personal data and privacy, are protected in the EU. These rights also apply in the digital environment. In 2025, almost six out of ten (59%) of EU citizens is aware that these rights that apply offline should also be respected online. Nevertheless, it shows digital rights are not commonly known by everyone and not all EU citizens take their digital rights for granted. In particular the 3 percentage point decrease compared to 2024 (62%) is worrying, albeit still higher than in 2023 (57%).<sup>16</sup>

Based on the Berlin Declaration Monitoring Mechanism, it seems that governments to a large extent consider *Commitment 1c. fostering and ensuring responsible and diligent action by all actors, public and private, in the digital environment*. From the EU27 Member States, in 2023, the implementation level of platforms to exchange and further develop national strategies with regard to digital transformation was self-reported by government representatives at 98%. Similarly, strategic projects with the aim of increasing awareness of the relevance of a value-based digital transformation were considered to be at an average completion level of 94%. Yet slightly lower, initiatives promoting the set-up of ethical and technological expert councils to provide advice to, and foster debate among citizens was implemented for 78% according to civil servants. These numbers were rather similar compared to 2022 (showing small increases and decreases with 96%, 96% and 83% respectively).<sup>17</sup>

No relevant data is available at the moment for *Commitment 1d. actively promoting this vision of the digital transformation, also in our international relations*. Thus, it is unclear how duty-bearers and rights-holders experience and value the implementation initiatives in this area.

---

<sup>15</sup> Special Eurobarometer 532, 551 and 103.2 on the Digital Decade, <https://europa.eu/eurobarometer/surveys/detail/3174>

<sup>16</sup> Special Eurobarometer 532, 551 and 103.2 on the Digital Decade, <https://europa.eu/eurobarometer/surveys/detail/3174>

<sup>17</sup> Berlin Declaration Monitoring Mechanism, [https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM\\_Report\\_2023\\_vFinal\\_rev.pdf](https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf)

## 4.2. Solidarity and inclusion (Declaration Chapter II)

**At the heart of the EU’s vision for a fair and inclusive digital future lies a commitment to solidarity and ensuring no one is left behind. This means creating digital spaces where every individual—regardless of their circumstances—can participate, learn, and thrive. The story below is a testament to how these values could come to life in a world that is still working toward full digital inclusion.**

### *Jakub*

*Jakub is a passionate community leader in a vibrant multicultural city in Europe, where he is actively involved in initiatives to support refugees and marginalised groups. One of his main struggles is ensuring that these communities can access essential services like healthcare, education, and legal aid, which increasingly depend on digital platforms. He notices that while there are many efforts to create inclusive digital environments, there are still too many gaps. For example, public services often fail to provide multilingual support, and some online platforms are not accessible to people with disabilities. For Jakub, solidarity means more than just offering help; it means creating an inclusive digital space where no one is left behind.*

Jakub’s story reflects the broader reality of digital transformation in the EU. It is not just about expanding access to technology but about fostering an environment where every individual, regardless of background or circumstance, can be part of the digital age. The EU’s dedication to solidarity and inclusion is key to ensuring that no one is excluded from the opportunities the digital world has to offer.

### 4.2.1. Implementation Initiatives

Across the EU27 Member States, 1245 initiatives can be linked to Solidarity and inclusion (Chapter II). In particular the following Sub-chapters, Principles and Commitments are covered by the implementation efforts:

<b>Solidarity and inclusion (Chapter II)</b>	<b>1245</b>
<b>Solidarity and inclusion (Chapter II)</b>	<b>302</b>
<i>Principle 2. Technology should be used to unite, and not divide, people. The digital transformation should contribute to a fair and inclusive society and economy in the EU.</i>	300
Commitment 2a. making sure that the design, development, deployment and use of technological solutions respect fundamental rights, enable their exercise and promote solidarity and inclusion	161
Commitment 2b. a digital transformation that leaves nobody behind. It should benefit everyone, achieve gender balance, and include notably elderly people, people living in rural areas, persons with disabilities, or marginalised, vulnerable or disenfranchised people and those who act on their behalf. It should also promote cultural and linguistic diversity	233
Commitment 2c. developing adequate frameworks so that all market actors benefiting from the digital transformation assume their social responsibilities	134

and make a fair and proportionate contribution to the costs of public goods, services and infrastructures, for the benefit of all people living in the EU.	
<b>Connectivity (Chapter II)</b>	<b>206</b>
<i>Principle 3. Everyone, everywhere in the EU, should have access to affordable and high-speed digital connectivity.</i>	206
Commitment 3a. ensuring access to high-quality connectivity, with available Internet access, for everyone wherever in the EU, including for those with low income.	163
Commitment 3b. protecting and promoting a neutral and open Internet where content, services, and applications are not unjustifiably blocked or degraded.	92
<b>Digital education, training and skills (Chapter II)</b>	<b>534</b>
<i>Principle 4. Everyone has the right to education, training and lifelong learning and should be able to acquire all basic and advanced digital skills.</i>	534
Commitment 4a. promoting high-quality digital education and training, including with a view to bridging the digital gender divide.	355
Commitment 4b. supporting efforts that allow all learners and teachers to acquire and share the necessary digital skills and competences, including media literacy, and critical thinking, to take an active part in the economy, society, and in democratic processes.	320
Commitment 4c. promoting and supporting efforts to equip all education and training institutions with digital connectivity, infrastructure and tools.	219
Commitment 4d. giving everyone the possibility to adjust to changes brought by the digitalisation of work through up-skilling and re-skilling.	262
<b>Fair and just working conditions (Chapter II)</b>	<b>160</b>
<i>Principle 5. Everyone has the right to fair, just, healthy and safe working conditions and appropriate protection in the digital environment as in the physical work place, regardless of their employment status, modality or duration.</i>	160
<i>Principle 6. Trade unions and employers' organisations play an important role in the digital transformation, particularly in relation to the definition of fair and just working conditions, including with regard to the use of digital tools at work.</i>	160
Commitment 5-6a. ensuring that everyone is able to disconnect and benefit from safeguards for work-life balance in a digital environment.	49
Commitment 5-6b. ensuring that, in the working environment, digital tools do not put workers' physical and mental health at risk in any way.	52
Commitment 5-6c. ensuring respect for workers' fundamental rights in the digital environment, including their right to privacy and the right to associate, right of collective bargaining and action, as well as protection against unlawful and unjustified surveillance.	35

Commitment 5-6d. ensuring that the use of artificial intelligence in the workplace is transparent and follows a risk-based approach and that corresponding prevention measures are taken to maintain a safe and healthy working environment.	74
Commitment 5-6e. ensuring in particular that human oversight is guaranteed in important decisions affecting workers, and that workers are generally informed that they are interacting with artificial intelligence systems.	71
<b>Digital public services online (Chapter II)</b>	<b>288</b>
<i>Principle 7. Everyone should have online access to key public services in the EU. Nobody is to be asked to provide data more often than necessary when accessing and using digital public services.</i>	288
Commitment 7a. 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.	173
Commitment 7b. ensuring wide accessibility and re-use of public sector information.	146
Commitment 7c. 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, including and in particular digital health and care services, notably access to electronic health records.	185

Table 4. Number of initiatives related to Solidarity and inclusion (Chapter II)

Initiatives in the area of **Solidarity and inclusion (Chapter II)** fulfil Commitments related to *Digital education, training and skills (Chapter II)*, especially in order to improve *Commitment 4a. promoting high-quality digital education and training, including with a view to bridging the digital gender divide*. Similarly to the previous Declaration Chapter, most of the initiatives are led by government organisations (1093, compared to 100 civil society, 51 industry initiatives and 1 from National Human Rights Institutions). Initiatives are predominantly policy related (316), followed by educational measures (284) and research and technology projects (273). Next to 1113 national initiatives, this Declaration Chapter is supported by relatively many city initiatives, 45. From a historical point of view, most initiatives started in 2023, with 260 new initiatives launched.

## Cyprus Good Practice – All Digital

- **Objectives:** To enhance digital skills among Cypriot citizens and businesses, focusing on areas such as basic digital literacy, coding, employability, entrepreneurship, STEAM education, and digital media literacy (2010 – Ongoing).
- **Description:** The Cyprus Computer Society organises initiatives like the BEBRAS Challenge, promoting informatics and computational thinking among students of all ages.
- **Stakeholder benefits:** Educational institutions and organisations benefit from structured programs that enhance teaching methodologies in digital competencies. Citizens gain improved digital skills, increasing their employability and ability to participate in the digital economy.
- **Accelerating mechanisms:** Strong collaboration between government bodies, educational institutions, and non-profit organisations ensures comprehensive and inclusive digital education initiatives.
- **Declaration Sub-chapters:** Digital education, training and skills (Chapter II).
- **Link for more information:** <https://digitalcoalition.gov.cy/initiative/all-digital-2/>.



### SOLIDARITY AND INCLUSION

Technology should unite,  
not divide, people.  
Everyone should have access  
to the internet, to digital  
skills, to digital public services,  
and to fair working conditions.

## Czechia Good Practice – ePrescription

- **Objectives:** To enhance patient convenience and safety by enabling cross-border electronic prescription (ePrescription) services, allowing Czech patients to obtain prescribed medications in participating European countries (2018 – Ongoing).
- **Description:** Czechia successfully integrated into the cross-border ePrescription network, starting with Poland as the first country where Czech patients could retrieve their ePrescriptions abroad. Subsequently, this service expanded to Croatia on June 26, 2023, and Spain on August 23, 2023.
- **Stakeholder benefits:** Healthcare providers benefit from streamlined prescription processes and improved data accuracy through electronic records. Patients experience increased convenience by accessing prescribed medications while traveling within participating countries, ensuring continuity of care.
- **Accelerating mechanisms:** Strong government support, EU-standard integration, robust eHealth infrastructure, collaboration with healthcare providers, and user-friendly implementation.
- **Declaration Sub-chapters:** Digital public services online (Chapter II).
- **Link for more information:** <https://epreskripce.gov.cz/o-ereceptu/about-prescription/>.



### SOLIDARITY AND INCLUSION

Technology should unite,  
not divide, people.  
Everyone should have access  
to the internet, to digital  
skills, to digital public services,  
and to fair working conditions.

## Greece Good Practice – Supply and Installation of Interactive Systems

- **Objectives:** To enhance the digital transformation of education by integrating interactive systems into classrooms, fostering a student-centred approach and collaborative learning (2021 – Ongoing).
- **Description:** This initiative involves the supply and installation of interactive learning systems in school units across Greece. The project aims to modernise the educational process by incorporating new technologies, thereby improving the pedagogical use of ICT in education. The infrastructure installed will support interactive and collaborative learning environments.
- **Stakeholder benefits:** Internally, teachers benefit from advanced teaching tools that facilitate interactive and engaging lessons. Externally, students gain from a more dynamic and collaborative learning experience, which can improve their digital skills and overall academic performance.
- **Accelerating mechanisms:** Effective integration of interactive systems into the existing curriculum, continuous training and support for teachers to maximise the use of new technologies, and collaboration with stakeholders to ensure the systems meet educational needs and standards.
- **Declaration Sub-chapters:** Digital education, training and skills (Chapter II).
- **Link for more information:** <https://digitalstrategy.gov.gr/en/projects/catalog>.



### SOLIDARITY AND INCLUSION

Technology should unite,  
not divide, people.  
Everyone should have access  
to the internet, to digital  
skills, to digital public services,  
and to fair working conditions.

## Denmark Good Practice – Broadband Pool

- **Objectives:** To extend high-speed internet access (minimum 100 Mbps) to rural areas of Denmark lacking sufficient coverage due to limited market incentives (2016 – Ongoing).
- **Description:** Provides financial support to households and businesses in underserved rural regions to establish very high-speed internet connections.
- **Stakeholder benefits:** Government agencies can achieve national digitalisation goals and promote regional development. Residents and businesses in rural areas gain access to high-speed internet, enhancing opportunities for education, work, and economic growth.
- **Accelerating mechanisms:** The program's success is driven by targeted funding, collaboration with local communities, and a focus on areas with inadequate market-driven broadband deployment.
- **Declaration Sub-chapters:** Connectivity (Chapter II).
- **Link for more information:** [https://commission.europa.eu/projects/broadband-pool\\_en](https://commission.europa.eu/projects/broadband-pool_en).



### SOLIDARITY AND INCLUSION

Technology should unite,  
not divide, people.  
Everyone should have access  
to the internet, to digital  
skills, to digital public services,  
and to fair working conditions.

## Spain Good Practice – BcnFem Tech

- **Objectives:** To promote gender equity in the tech sector by supporting women-led projects and bridging the digital gender divide in Barcelona (2021 – Ongoing).
- **Description:** Includes a training program and awards to empower women in technology.
- **Stakeholder benefits:** The city government advances its gender equity goals and fosters a more inclusive tech ecosystem. Women gain skills, recognition, and support, enhancing their participation in the tech industry.
- **Accelerating mechanisms:** Strong public-private partnerships, targeted training programs, and dedicated awards.
- **Declaration Sub-chapters:** Solidarity and inclusion; Digital education, training and skills (Chapter II).
- **Link for more information:** <https://ajuntament.barcelona.cat/digital/en/technology-accessible-everyone/fight-against-digital-inequality/fight-against-digital-inequality-1>.



### SOLIDARITY AND INCLUSION

Technology should **unite**,  
not **divide**, people.  
Everyone should have access  
to the internet, to digital  
skills, to digital public services,  
and to fair working conditions.

## 4.2.2. Impact Indicators and Visible Results

As far as the area of **Solidarity and inclusion (Chapter II)** is concerned the public sector demonstrates various efforts, for instance to support *Commitment 2a. making sure that the design, development, deployment and use of technological solutions respect fundamental rights, enable their exercise and promote solidarity and inclusion*. Efforts to include fundamental rights principles in public innovation policies has succeeded for 68% according to public officials in 2023, the same completion rate as in 2022.<sup>18</sup> To a larger extent fundamental rights principles have been included in technology procurement rules, with 79% in 2023, despite completion being at 81% in 2022.<sup>19</sup> Another relevant finding is that just 45% of all government portals in the EU27 Member States provide information on how users can enrol in any activity to improve the design and delivery of services.<sup>20</sup> Overlooking these findings, fundamental rights and technological solutions do not yet fully go hand in hand from a participative point of view.

Digital rights should apply to all, without discrimination and bias, as articulated in *Commitment 2b. a digital transformation that leaves nobody behind. It should benefit everyone, achieve gender balance, and include notably elderly people, people living in rural areas, persons with disabilities, or marginalised, vulnerable or disenfranchised people and those who act on their behalf. It should also promote cultural and linguistic diversity*. This Commitment can partly be evaluated based on internet usage statistics. Internet usage figures demonstrate that gaps between different societal groups are not visible in all ways.<sup>21</sup> On average, 91% of the persons living in rural areas used the internet in 2024, compared to the population on average (94%). Slightly lower online usage goes for elderly in the age of 55 to 74 years old (86%) and persons with a limited disability (89%), indicating that so far

<sup>18</sup> Berlin Declaration Monitoring Mechanism, [https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM\\_Report\\_2023\\_vFinal\\_rev.pdf](https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf)

<sup>19</sup> Berlin Declaration Monitoring Mechanism, [https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM\\_Report\\_2023\\_vFinal\\_rev.pdf](https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf)

<sup>20</sup> Berlin Declaration Monitoring Mechanism, [https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM\\_Report\\_2023\\_vFinal\\_rev.pdf](https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf)

<sup>21</sup> [https://ec.europa.eu/eurostat/databrowser/view/isoc\\_ci\\_ifp\\_iu\\_custom\\_15159133/default/table?lang=en](https://ec.europa.eu/eurostat/databrowser/view/isoc_ci_ifp_iu_custom_15159133/default/table?lang=en)

not everyone in the EU takes part in online activities and benefits from the digital transformation. Instead, women in the age of 25 to 64 show are above the average internet usage (98%). Moreover, the eGovernment Benchmark shows that at least 65% of all government websites and portals fails to meet a selection of web accessibility criteria covered by the Web Accessibility Directive.<sup>22</sup>

No relevant data is available at the moment for *Commitment 2c. developing 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 infrastructures, for the benefit of all people living in the EU*. It is unclear how different actors take adequate measures.

The digital right to **Connectivity (Chapter II)** is respected through actions such as *Commitment 3a. ensuring access to high-quality connectivity, with available Internet access, for everyone wherever in the EU, including for those with low income*. Various statistics point out the status. On average, the EU27 Member States had varying levels of connectivity in 2023, with 79% of the EU households connected with Fixed Very High Capacity Network (VHCN), 64% Fibre to the Premises (FTTP) coverage, 19% share of fixed broadband subscriptions  $\geq 1$  Gbps, and 89% overall 5G coverage.<sup>23</sup> Rights-holders in the EU have a less optimistic view, with ample room for improvement. Across the EU27, 57% feels their right for getting an affordable high-speed internet connection is well respected in 2025, unchanged from 57% in 2024 but improved from 53% in 2023.<sup>24</sup> No information is available on how everyone is benefitting from such digital infrastructure, such as persons with low income.

No data can be provided for *Commitment 3b. protecting and promoting a neutral and open Internet where content, services, and applications are not unjustifiably blocked or degraded*.

When it comes to the area of **Digital education, training and skills (Chapter II)** Member States actively progress in areas, such as *Commitment 4a. promoting high-quality digital education and training, including with a view to bridging the digital gender divide*. Member States actions for the promotion of digital skills and awareness in the public sector was assessed with a completion rate of 71% in 2023, even though in 2022 this was considered fully completed at 100%.<sup>25</sup> Actual digital skills levels are not yet fully developed. Looking at individuals with basic or above basic overall digital skills, gender divides are apparent to a limited extent only. In fact, such digital skills levels were present among 54% of women in 2023, compared to 56% in the entire EU population.<sup>26</sup> This is also reflected in perceptions of EU persons regarding these digital rights and principles. In 2025, 60% believes that their rights to getting basic and advanced digital education, training and skills are respected. In 2024 and 2023 these numbers were at 60% and 56%.<sup>27</sup> Even though the jump from 2023 to 2024 is not repeated and opportunities for growth remain plentiful, digital education rights are among the best protected digital rights according to EU citizens.

There are indications that the digital rights and principles are less respected in case of *Commitment 4b. supporting efforts that allow all learners and teachers to acquire and share the necessary digital skills and competences, including media literacy, and critical thinking, to take an active part in the economy, society, and in democratic processes*. In both 2023

---

<sup>22</sup> eGovernment Benchmark, <https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-egovernment-benchmark>

<sup>23</sup> <https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-broadband-coverage-europe-2023>

<sup>24</sup> Special Eurobarometer 532, 551 and 103.2 on the Digital Decade, <https://europa.eu/eurobarometer/surveys/detail/3174>

<sup>25</sup> Berlin Declaration Monitoring Mechanism, [https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM\\_Report\\_2023\\_vFinal\\_rev.pdf](https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf)

<sup>26</sup> [https://ec.europa.eu/eurostat/databrowser/view/sdg\\_04\\_70/default/table](https://ec.europa.eu/eurostat/databrowser/view/sdg_04_70/default/table)

<sup>27</sup> Special Eurobarometer 532, 551 and 103.2 on the Digital Decade, <https://europa.eu/eurobarometer/surveys/detail/3174>

and 2021 only one quarter (24%) of EU persons had checked the truthfulness of the information or content they found on the internet news sites or social media in the last 3 months prior to answering this question in a survey.<sup>28</sup> Whenever checking the truthfulness of information online signals lacking skills for media literacy and critical thinking, this could in the end negatively impact people's ability to take active part in the economy, society and democracy. At the same time there could be many reasons for the fact that people do not check, including that they can trust information and believe that they only use reliable sources.

A mixed picture is visible for *Commitment 4c. promoting and supporting efforts to equip all education and training institutions with digital connectivity, infrastructure and tools*. In 2017-2018, 53% of students attended highly digitally equipped and connected schools.<sup>29</sup> In 2023, equally, 53% of the students attended schools whose ICT coordinator indicated availability of access to Wi-Fi, space on a school network to store files, remote access to the school network from home, a learning management system, 3D printers, programmable robots or robotic devices.<sup>30</sup>

In terms of digital up-skilling, 40% of persons working in the EU learned to use any new computer programs or software to do their main job in 2021 or since they started their main job.<sup>31</sup> This partially favours the *Commitment 4d. giving everyone the possibility to adjust to changes brought by the digitalisation of work through up-skilling and re-skilling*.

Furthermore, the area of **Fair and just working conditions (Chapter II)** ensures actions, such as the *Commitment 5-6a. ensuring that everyone is able to disconnect and benefit from safeguards for work-life balance in a digital environment*. Member States report to have completed 87% of their efforts in setting up guidelines on healthy and appropriate use of technologies in the workplace, to prevent adverse impact on mental or physical human health development (in 2023, as was the case in 2022).<sup>32</sup> From a rights-holders perspective, such digital rights are less embedded. In 2025, 54% argues that fair and healthy working conditions in the digital environment, including the work-life balance are respected. This ends the upward trend reached with 55% in 2024 compared to 51% in 2023.<sup>33</sup>

Rights-holders have a similar view on *Commitment 5-6c. ensuring respect for workers' fundamental rights in the digital environment, including their right to privacy and the right to associate, right of collective bargaining and action, as well as protection against unlawful and unjustified surveillance*. In 2025, 2024 and 2023, respectively 59%, 59% and 60% of the EU population felt their digital rights and principles were applied in their country for getting freedom of assembly and association in the digital environment.<sup>34</sup> Although citizens consider these work-related digital rights to be among the most protected digital rights in the EU, the flat numbers question whether progress stagnates. In 2019, 73% of the EU companies refrained from using data analytics for monitoring employee performance.<sup>35</sup> The remaining quarter has used monitoring performance with analytical tooling, yet it is unclear whether these can be considered as unlawful or unjustified surveillance in any way.

---

<sup>28</sup>

[https://ec.europa.eu/eurostat/databrowser/view/ISOC\\_SK\\_EDIC\\_I21\\_custom\\_15160321/default/table?lang=en&page=time:2023](https://ec.europa.eu/eurostat/databrowser/view/ISOC_SK_EDIC_I21_custom_15160321/default/table?lang=en&page=time:2023)

<sup>29</sup> <https://digital-strategy.ec.europa.eu/en/library/2nd-survey-schools-ict-education-0>

<sup>30</sup> Numbers for 21 EU Member States, [https://www.iea.nl/sites/default/files/2024-11/ICILS\\_2023\\_International\\_Report\\_0.pdf](https://www.iea.nl/sites/default/files/2024-11/ICILS_2023_International_Report_0.pdf)

<sup>31</sup> <https://www.cedefop.europa.eu/en/tools/european-skills-jobs-survey/data/explorer?country=EU27&field12=A1&indicator=Q38T95#1>

<sup>32</sup> Berlin Declaration Monitoring Mechanism, [https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM\\_Report\\_2023\\_vFinal\\_rev.pdf](https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf)

<sup>33</sup> Special Eurobarometer 532, 551 and 103.2 on the Digital Decade, <https://europa.eu/eurobarometer/surveys/detail/3174>

<sup>34</sup> Special Eurobarometer 532, 551 and 103.2 on the Digital Decade, <https://europa.eu/eurobarometer/surveys/detail/3174>

<sup>35</sup> <https://www.eurofound.europa.eu/en/data-catalogue/european-company-survey>

No data was found for *Commitment 5-6b. ensuring that, in the working environment, digital tools do not put workers' physical and mental health at risk in any way, Commitment 5-6d. ensuring that the use of artificial intelligence in the workplace is transparent and follows a risk-based approach and that corresponding prevention measures are taken to maintain a safe and healthy working environment*, neither is data available for *Commitment 5-6e. ensuring in particular that human oversight is guaranteed in important decisions affecting workers, and that workers are generally informed that they are interacting with artificial intelligence systems*.

Next, everyone in the EU deserves **Digital public services online (Chapter II)**, including *Commitment 7a. 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*. Relevant in this regard is that persons in the EU can use their notified national eID to authenticate for 76% of online government services.<sup>36</sup> Moreover, Member States declared in 2023 that all have notified at least one of their national eID schemes to the European Commission, compared to 73% in 2022.<sup>37</sup> Actions to provide private sector bodies with incentives to use European trustworthy and notified eIDs are considered at a completion level of 83% in 2023, jumping from 56% in 2022.<sup>38</sup> Member States also indicated to meet the requirements set by the Single Digital Gateway Regulation on the online availability and accessibility of the administrative procedures for 93% in 2023, 87% in 2022.<sup>39</sup> From a rights-holders point of view, the perception of these digital rights and principles is lower than the self-reported provision level by Member States. When it comes to getting easy online access to all key public services in the EU, 58% of the EU population trusts this digital right to be granted in 2025, compared to 58% in 2024, 54% in 2023.<sup>40</sup> Reversely, four out of ten citizens feel their right to key public services is overlooked. Thus, there is no room for complacency. The more so, because the upward trend since 2023 seems to plateau.

Several accomplishments can be seen in the area of *Commitment 7b. ensuring wide accessibility and re-use of public sector information*. This is reflected by the overall Open Data Maturity average composite score of 83% in 2024 (similar to 2023).<sup>41</sup> More specifically, Member States consider their strategies and policies outlining measures supporting the re-use of open data by the public sector to be at a completion level of 96% in 2023, 89% in 2022. Government representatives also indicated that all Member States have open data portals, via which open data can be easily found through one central place for re-use purposes.<sup>42</sup>

Public healthcare services are among the services that may affect persons living in the EU most, as stated in *Commitment 7c. 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, including and in particular digital health and care services, notably access to electronic health records*. The overall access to e-health records composite score stood at 79% by the end of 2023, with 72% in 2022.<sup>43</sup>

---

<sup>36</sup> <https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-egovernment-benchmark>

<sup>37</sup> Berlin Declaration Monitoring Mechanism, [https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM\\_Report\\_2023\\_vFinal\\_rev.pdf](https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf)

<sup>38</sup> Berlin Declaration Monitoring Mechanism, [https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM\\_Report\\_2023\\_vFinal\\_rev.pdf](https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf)

<sup>39</sup> Berlin Declaration Monitoring Mechanism, [https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM\\_Report\\_2023\\_vFinal\\_rev.pdf](https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf)

<sup>40</sup> Special Eurobarometer 532, 551 and 103.2 on the Digital Decade, <https://europa.eu/eurobarometer/surveys/detail/3174>

<sup>41</sup> <https://data.europa.eu/en/publications/open-data-maturity>

<sup>42</sup> Berlin Declaration Monitoring Mechanism, [https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM\\_Report\\_2023\\_vFinal\\_rev.pdf](https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf)

<sup>43</sup> <https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-ehealth-indicator-study>

### 4.3. Freedom of choice (Declaration Chapter III)

**At the core of the EU’s vision for a fair digital future is the principle of enabling freedom of choice for everyone. This means designing systems that offer equal opportunities, no matter a person’s background or location. The story below highlights how, when AI is not carefully designed, it could unintentionally limit individuals’ ability to access opportunities.**

#### *Priya*

*Priya works at a medium-sized company that uses AI to screen candidates, aiming to make hiring decisions faster and more efficient. However, she notices that the AI algorithm seems to prioritise applicants living closer to the office, unintentionally excluding qualified candidates from rural areas who are willing to relocate or work remotely. Priya’s story highlights the need for AI systems to support true freedom of choice; offering all candidates an equal opportunity to apply, regardless of their location. It calls for AI technology that is not only fair, accountable, and transparent but also ensures that digital systems do not restrict individuals’ ability to pursue opportunities based on arbitrary factors.*

Priya’s story highlights the need for digital systems that exclude any bias or discrimination. Digital products and services are to be designed with fairness and inclusivity in mind, ensuring that everyone has the freedom to choose without facing unintentional barriers. It is essential that technology empowers individuals, offering equal opportunities for all, regardless of where they live or their circumstances.

#### 4.3.1. Implementation Initiatives

Across the EU27 Member States, 282 initiatives can be linked to **Freedom of choice (Chapter III)**. In particular the following Sub-chapters, Principles and Commitments are covered by the implementation efforts:

<b>Freedom of choice (Chapter III)</b>	<b>282</b>
<b>Interactions with algorithms and artificial intelligence systems (Chapter III)</b>	<b>195</b>
<i>Principle 8. Artificial intelligence should serve as a tool for people, with the ultimate aim of increasing human well-being.</i>	195
<i>Principle 9. Everyone should be empowered to benefit from the advantages of algorithmic and artificial intelligence systems including by making their own, informed choices in the digital environment, while being protected against risks and harm to one’s health, safety and fundamental rights.</i>	195
Commitment 8-9a. promoting human-centric, trustworthy and ethical artificial intelligence systems throughout their development, deployment and use, in line with EU values.	185
Commitment 8-9b. ensuring an adequate level of transparency about the use of algorithms and artificial intelligence, and that people are empowered to use them and are informed when interacting with them.	185

Commitment 8-9c. ensuring that algorithmic systems are based on adequate datasets to avoid discrimination and enable human supervision of all outcomes affecting people's safety and fundamental rights.	175
Commitment 8-9d. ensuring that technologies such as artificial intelligence are not used to pre-empt people's choices, for example regarding health, education, employment, and their private life.	178
Commitment 8-9e. providing for safeguards and taking appropriate action, including by promoting trustworthy standards, to ensure that artificial intelligence and digital systems are, at all times, safe and used in full respect for fundamental rights.	177
Commitment 8-9f. taking measures to ensure that research in artificial intelligence respects the highest ethical standards and relevant EU law.	177
<b>A fair digital environment (Chapter III)</b>	<b>137</b>
<i>Principle 10. Everyone should be able to effectively and freely choose which online services to use, based on objective, transparent, easily accessible and reliable information.</i>	137
<i>Principle 11. Everyone should have the possibility to compete fairly and innovate in the digital environment. This should also benefit businesses, including SMEs.</i>	137
Commitment 10-11a. ensuring a safe and secure digital environment based on fair competition, where fundamental rights are protected, users rights and consumer protection in the Digital Single Market are ensured, and responsibilities of platforms, especially large players and gatekeepers, are well defined.	99
Commitment 10-11b. promoting interoperability, transparency, open technologies and standards as a way to further strengthen trust in technology as well as consumers' ability to make autonomous and informed choices.	123

Table 5. Number of initiatives related to Chapter III. Freedom of choice

Initiatives around **Freedom of choice (Chapter III)** are evenly distributed across the area of *Interactions with algorithms and AI systems (Chapter III)* and *A fair digital environment (Chapter III)*. Initiatives are led by government organisations (243, compared to 22 civil society, 13 industry initiatives and 3 initiatives from National Human Rights Institutions). Initiatives are predominantly policy related (91) or implementing research and technology solutions (75). Next to 228 national initiatives, this Declaration Chapter is supported with 33 local initiatives. From a historical point of view, most initiatives started in 2024, with 54 initiatives launched and showing digital rights in this field seem to be on the rise. More recent initiatives may have derived from the AI Act, which entered into force on 1 August 2024 and relates to the digital rights and principles to be respected based on this Declaration Chapter.<sup>44</sup>

<sup>44</sup> <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

## Austria Good Practice – Practical Guide for Digital Administration: AI, Ethics and Law 2.0

- **Objectives:** Published in 2024, the guide aims to provide public administrations in Austria with a structured framework for the ethical, legal, and practical implementation of AI in public services, ensuring transparency, accountability, and compliance with fundamental rights.
- **Description:** Developed as a comprehensive resource for policymakers and public officials, the guide outlines best practices for responsible AI deployment in digital administration. It covers key areas such as risk assessment, bias mitigation, data protection, and ethical considerations to ensure AI systems align with democratic values and legal standards.
- **Stakeholder benefits:** Public administrators gain access to practical guidelines and legal insights to support responsible AI adoption. Citizens benefit from enhanced transparency, fairness, and accountability in AI-driven public services, ensuring trust in digital governance.
- **Accelerating mechanisms:** Strong alignment with EU regulations and ethical AI principles, collaboration between government agencies, legal experts, and technology specialists, and the development of standardized frameworks to guide AI implementation in public services.
- **Declaration Sub-chapters:** Interactions with algorithms and artificial intelligence systems (Chapter III)
- **Link for more information:** <https://oeffentlicherdienst.gv.at/verwaltungsinnovation/public-management-und-governance/digitale-verwaltung/praxisleitfaden-digitale-verwaltung-und-ethik/>



### FREEDOM OF CHOICE

People should benefit from a fair online environment, be safe from illegal and harmful content, and be empowered when they interact with new and evolving technologies like artificial intelligence.

## Estonia Good Practice – Digital Transformation for SMEs

- **Objectives:** Aims to enhance the digital capabilities of small and medium-sized enterprises (SMEs) by providing access to advanced technologies, fostering innovation, and improving competitiveness in the digital economy. In 2023 the National Digital Decade Strategic Roadmap was introduced outlining its visions for digital transformation by 2030 (2000 – Ongoing).
- **Description:** Estonia supports SMEs in digital transformation through access to digital tools, training programs, and collaborations with tech providers.
- **Stakeholder benefits:** Government agencies benefit from a more robust and innovative SME sector, contributing to economic growth and job creation. SMEs gain improved access to digital tools and expertise, leading to increased efficiency, market reach, and competitiveness.
- **Accelerating mechanisms:** Strong government support, a culture of innovation, and a collaborative ecosystem that includes public institutions, private companies, and educational organisations.
- **Declaration Sub-chapters:** Digital education, training and skills (Chapter II); Solidarity and inclusion (Chapter II); A fair digital environment (Chapter III)
- **Link for more information:** <https://e-estonia.com/>.



### FREEDOM OF CHOICE

People should benefit from a fair online environment, be safe from illegal and harmful content, and be empowered when they interact with new and evolving technologies like artificial intelligence.

## Netherlands Good Practice – Interprovincial Guide Digital Ethics

- **Objectives:** To develop a practical guide by which the 12 provinces in the Netherlands can address ethical challenges, including those related to digital rights and the responsible use of AI and algorithms (2024 - Ongoing).
- **Description:** The Association of Provinces of the Netherlands (IPO) published a guide on digital ethics, emphasizing transparency and accountability in AI and algorithm deployment. An updated version was launched in 2024.
- **Stakeholder benefits:** The role of provinces on digital topics is growing. This guide supports employees at the 12 provinces and beneficiaries of their policies by ensuring ethical, transparent, and accountable use of digital technologies, particularly AI and algorithms.
- **Accelerating mechanisms:** Collaboration among civil servants from all 12 provinces and leveraging tools from internal and external experts.
- **Declaration Sub-chapters:** Solidarity and inclusion (Chapter II); Interactions with algorithms and artificial intelligence systems (Chapter III); Privacy and individual control over data (Chapter V); Sustainability (Chapter VI).
- **Link for more information:** <https://www.ipo.nl/media/orqpqbf1/de-interprovinciale-gids-digitale-ethiek-08112024.pdf>.



### FREEDOM OF CHOICE

People should benefit from a fair online environment, be safe from illegal and harmful content, and be empowered when they interact with new and evolving technologies like artificial intelligence.

## Malta Good Practice – Digital Innovation Hub

- **Objectives:** To empower individuals and workforces across various sectors with cutting-edge digital competencies, addressing the evolving demands of the digital age (2024-Ongoing).
- **Description:** The DiHubMT provides a comprehensive set of services as a European Digital Innovation Hub (EDIH), offering support to SMEs, small midcaps, and public sector organisations in Malta.
- **Stakeholder benefits:** Access to advanced technologies and professional support enhances innovation and competitiveness. SMEs and start-ups benefit from resources like 3D printers, podcasting studios, and metaverse platforms, fostering business growth.
- **Accelerating mechanisms:** Collaboration with local tech companies, partnerships with EU innovation networks, and the provision of state-of-the-art facilities (e.g., 3D printers, AI platforms) for hands-on development and experimentation.
- **Declaration Sub-chapters:** Digital education, training and skills (Chapter II); A fair digital environment (Chapter III).
- **Link for more information:** <https://dihubmt.eu/>.



### FREEDOM OF CHOICE

People should benefit from a fair online environment, be safe from illegal and harmful content, and be empowered when they interact with new and evolving technologies like artificial intelligence.

## Slovenia Good Practice – T-2 Smart Cities 4.0

- **Objectives:** To enhance urban living through the integration of advanced Internet of Things (IoT) technologies, promoting sustainable development, efficient public services, and active citizen engagement in Slovenian municipalities (2022 – Ongoing).
- **Description:** Led by T-2 d.o.o. in collaboration with partners like Solviks d.o.o. and Flycom Technologies d.o.o., the T-2 Smart Cities 4.0 project aims to develop a comprehensive platform connecting smart cities and communities. The initiative involves integrating IoT sensor technologies, car-sharing systems, and citizen connectivity platforms. This platform enables municipalities to communicate directly with citizens via a mobile app, providing real-time information on events, public services, traffic, parking, and air quality.
- **Stakeholder benefits:** Municipalities benefit from improved public service delivery and enhanced citizen engagement through real-time data and communication channels. Citizens gain access to timely information, contributing to a better quality of life and increased participation in community activities. The integration of sustainable technologies also supports environmental goals.
- **Accelerating mechanisms:** Collaboration among local governments, local providers and citizens and funding.
- **Declaration Sub-chapters:** Digital education, training and skills (Chapter II); A fair digital environment (Chapter III).
- **Link for more information:** <https://www.smartcity.si/en/>.



### FREEDOM OF CHOICE

People should benefit from a fair online environment, be safe from illegal and harmful content, and be empowered when they interact with new and evolving technologies like artificial intelligence.

### 4.3.2. Impact Indicators and Visible Results

Impact seems to come with certain hesitance in the area of **Interactions with algorithms and AI systems (Chapter III)**. Within the public sector this has been visible by self-reported implementation levels of 53% in 2022 and 61% in 2023 for Member States sharing best practices on the development of successful human-centric AI systems in the public sector that can be used by all public administrations at European, national and subnational levels.<sup>45</sup> This pinpoints progress and at the same time argues for additional efforts around *Commitment 8-9a. promoting human-centric, trustworthy and ethical artificial intelligence systems throughout their development, deployment and use, in line with EU values.*

A similar observation can be made for *Commitment 8-9b. ensuring an adequate level of transparency about the use of algorithms and artificial intelligence, and that people are empowered to use them and are informed when interacting with them.* As indicated by the transparency with regards to automated decision-making processes used in digital public services, implementation levels have been at 57% in 2022 and 64% in 2023 according to the EU27 Member States.<sup>46</sup>

The Declaration also seeks to protect free choices by rights-holders in the digital age, as noted in *Commitment 8-9d. ensuring that technologies such as artificial intelligence are not used to pre-empt people's choices, for example regarding health, education, employment, and their private life.* About half of the EU population (53% in 2025, 52% in 2024, 49% in

<sup>45</sup> Berlin Declaration Monitoring Mechanism, [https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM\\_Report\\_2023\\_vFinal\\_rev.pdf](https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf)

<sup>46</sup> Berlin Declaration Monitoring Mechanism, [https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM\\_Report\\_2023\\_vFinal\\_rev.pdf](https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf)

2023) believes that they get effective freedom of choice online, also when interacting with artificial intelligence.<sup>47</sup> Given the relative slow rise in recent years, it may be asked whether enough is done and/or whether citizens perceive the actual efforts taking place in this area.

It seems that standardisation is one way duty-bearers promote fair interactions with algorithms and AI, linking to *Commitment 8-9e. providing for safeguards and taking appropriate action, including by promoting trustworthy standards, to ensure that artificial intelligence and digital systems are, at all times, safe and used in full respect for fundamental rights*. Although numbers are not available for the private sector, the use of quality standards of data sets to feed into AI systems when designing digital public services is considered to be at a completion level of two thirds (73% in 2022, 74% in 2023) across the EU27 Member States.<sup>48</sup>

For the other related Commitments no relevant data was found (*Commitment 8-9c. ensuring that algorithmic systems are based on adequate datasets to avoid discrimination and enable human supervision of all outcomes affecting people's safety and fundamental rights; Commitment 8-9f. taking measures to ensure that research in artificial intelligence respects the highest ethical standards and relevant EU law*).

As for a **fair digital environment**, little is known about the impact and visible results for *Commitment 10-11a. ensuring a safe and secure digital environment based on fair competition, where fundamental rights are protected, users rights and consumer protection in the Digital Single Market are ensured, and responsibilities of platforms, especially large players and gatekeepers, are well defined*. Relevant though is the finding from 2020 that only 22% of 2,863 EU businesses and business users consulted during the public consultation on the Digital Services Act Package had encountered fair trading conditions on large platforms.<sup>49</sup> Others were affected by unfair practices by large gatekeeper platforms such as exclusionary conducts, exploitative conducts and transparency-related problems.

When looking at the deployment of 18 key internet standards it becomes clear that further actions could strengthen the realisation of *Commitment 10-11b. promoting interoperability, transparency, open technologies and standards as a way to further strengthen trust in technology as well as consumers' ability to make autonomous and informed choices*. Across EU websites and domains tested in 2024, 62% complied with standards for browsing (web communication standards), routing (MANRS), emailing (email communication security standards), naming (DNSSEC) and addressing (IPv6).<sup>50</sup>

---

<sup>47</sup> Special Eurobarometer 532, 551 and 103.2 on the Digital Decade, <https://europa.eu/eurobarometer/surveys/detail/3174>

<sup>48</sup> Berlin Declaration Monitoring Mechanism, [https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM\\_Report\\_2023\\_vFinal\\_rev.pdf](https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf)

<sup>49</sup> <https://digital-strategy.ec.europa.eu/en/library/summary-report-open-public-consultation-digital-services-act-package>

<sup>50</sup> <https://ec.europa.eu/internet-standards/>

## 4.4. Participation in the digital public space (Declaration Chapter IV)

At the core of the EU's digital rights framework is the belief that citizens should have access to a trustworthy, diverse and multilingual online environment and should know who owns or controls the services they are using. This encourages pluralistic public debate and participation in democracy. Digital platforms should enable individuals to engage in discussions, challenge ideas, and voice dissent without compromising their privacy or personal security. Ensuring that freedom of expression thrives in the digital space requires not only robust data protection but also safeguards against undue content restrictions and online repression. The story below highlights the importance of protecting online freedom of expression as a fundamental pillar of digital democracy.

### *Eva*

*Eva, a university student passionate about social and political issues, frequently shares her views on climate action through online platforms. However, after posting a critical analysis of an environmental policy, she notices her content being flagged, its reach restricted, and some posts removed without clear explanation. At the same time, she becomes the target of online harassment, facing an influx of hostile messages and personal attacks. With no transparency about why her content is being suppressed and limited recourse to challenge these actions, Eva begins to question whether she can safely and freely express her opinions online.*

Eva's story underscores the critical need for digital platforms that uphold and protect freedom of expression online. For digital democracy to thrive, individuals must be able to share their views openly, challenge authority, and engage in public discourse without fear of censorship, intimidation, or retaliation. A truly democratic digital environment ensures that all voices can be heard while safeguarding users from both undue restrictions and online harassment.

### 4.4.1. Implementation Initiatives

Across the EU27 Member States, 239 initiatives can be linked to **Participation in the digital public space (Chapter IV)**. In particular the following Sub-chapters, Principles and Commitments are covered by the implementation efforts:

<b>Participation in the digital public space (Chapter IV)</b>	<b>239</b>
<i>Principle 12. Everyone should have access to a trustworthy, diverse and multilingual digital environment. Access to diverse content contributes to a pluralistic public debate and effective participation in democracy in a non-discriminatory manner.</i>	238
<i>Principle 13. Everyone has the right to freedom of expression and information, as well as freedom of assembly and of association in the digital environment.</i>	238
<i>Principle 14. Everyone should be able to access information on who owns or controls the media services they are using.</i>	239
<i>Principle 15. Online platforms, particularly very large online platforms, should support free democratic debate online. Given the role of their services in</i>	238

<i>shaping public opinion and discourse, very large online platforms should mitigate the risks stemming from the functioning and use of their services, including in relation to misinformation and disinformation campaigns, and protect freedom of expression.</i>	
Commitment 12-15a. continuing safeguarding all fundamental rights online, notably the freedom of expression and information, including media freedom and pluralism.	103
Commitment 12-15b. supporting the development and best use of digital technologies to stimulate people's engagement and democratic participation.	134
Commitment 12-15c. taking proportionate measures to tackle all forms of illegal content, in full respect for fundamental rights, including the right to freedom of expression and information, and without establishing any general monitoring obligations or censorship.	92
Commitment 12-15d. creating a digital environment where people are protected against disinformation and information manipulation and other forms of harmful content, including harassment and gender-based violence.	95
Commitment 12-15e. supporting effective access to digital content reflecting the cultural and linguistic diversity in the EU.	81
Commitment 12-15f. empowering individuals to make freely given, specific choices and limiting the exploitation of vulnerabilities and biases, namely through targeted advertising.	72

Table 6. Number of initiatives related to Participation in the digital public space (Chapter IV)

Within **Participation in the digital public space (Chapter IV)** efforts mostly contribute to *Commitment 12-15b. supporting the development and best use of digital technologies to stimulate people's engagement and democratic participation*, while least initiatives have been identified to support *Commitment 12-15f. empowering individuals to make freely given, specific choices and limiting the exploitation of vulnerabilities and biases, namely through targeted advertising*. are led by government organisations (183, compared to 44 civil society and 12 industry initiatives, as well as 1 from a National Human Rights Institution). Initiatives are predominantly research and technology solutions (53), as well as policy related (43) or legal (41). With 167 initiatives at the national level, 33 at the international level, 1 at the regional level, 39 at the local level, it is apparent that digital rights in this field are mostly promoted and protected nationally. From a historical point of view, most initiatives started in 2024, with 146 initiatives launched. Further national efforts may be expected following the Digital Services Act, which applies to all platforms as of 17 February 2024, including online marketplaces, social networks, content-sharing platforms, app stores and online travel and accommodation platforms.<sup>51</sup> The Digital Services Act incorporated mechanisms such as its trusted flaggers and “Code of Conduct on Countering Illegal Hate Speech Online +”, may equally foster new initiatives by government, civil society and industry stakeholders in the Member States.<sup>52</sup> To protect media freedom and pluralism

<sup>51</sup> [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en)

<sup>52</sup> <https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa>; <https://digital-strategy.ec.europa.eu/en/library/code-conduct-countering-illegal-hate-speech-online>

the European Media Freedom Act entered into force on 7 May 2024.<sup>53</sup> Again, such EU measure can fuel digital rights initiatives by a wide range of stakeholders in the coming time.

### Sweden Good Practice – Källkritikbyrån

- **Objectives:** Aims to strengthen critical thinking and source evaluation skills among the public, particularly targeting misinformation and disinformation online (2024 – Ongoing).
- **Description:** Källkritikbyrån is an independent initiative providing fact-checking, educational materials, and practical tools for assessing digital content. It conducts workshops, publishes analyses on misinformation trends, and collaborates with media and educational institutions to improve information literacy.
- **Stakeholder benefits:** Enhances awareness and ability to distinguish reliable from misleading content and provides teaching materials and strategies for integrating media literacy into curricula.
- **Accelerating mechanisms :** Strong partnerships, active engagements through social media and public campaigns, use of interactive tools and real-world case studies.
- **Link for more information:** <https://kallkritikbyran.se/>.



#### PARTICIPATION

Citizens should be able to engage in the democratic process at all levels, and have control over their own data.

### Hungary Good Practice – The Internet Hotline

- **Objectives:** To make the internet a safer place by providing an online information and assistance service where users can report illegal or harmful content, particularly content that is harmful to minors (2011 – Ongoing).
- **Description:** The Internet Hotline, operated by the National Media and Infocommunications Authority (NMHH) since 2011, allows users to report various types of harmful online content. These include child pornography, online harassment, racist content, incitement against a community, and other content harmful to minors. The service investigates reports and provides legal assistance and technical advice to protect public interests in the safe use of the internet.
- **Stakeholder benefits:** Internally, the NMHH benefits from enhanced capabilities to monitor and address harmful online content. Externally, the public, especially minors, benefit from a safer online environment and access to a reliable reporting mechanism for harmful content.
- **Accelerating mechanisms:** Key success factors include the ability to report content anonymously, collaboration with international partners through the INHOPE network, and the hotline's procedures and technologies to effectively handle reports.
- **Link for more information:** <https://www.internethotline.hu>.



#### PARTICIPATION

Citizens should be able to engage in the democratic process at all levels, and have control over their own data.

<sup>53</sup> [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/european-media-freedom-act\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/european-media-freedom-act_en)

## France Good Practice – Aide au pluralisme des services de presse tout en ligne – SPTTEL

- **Objectives:** To support the pluralism of online press services by providing financial aid to digital-only press services, ensuring the sustainability of their economic model and promoting access to quality journalism and diverse ideas (2021 – Ongoing).
- **Description:** The aid for the pluralism of online press services was established by decree n°2021-16666 on December 15, 2021. It targets press services that are exclusively distributed electronically, without any print format. The aid benefits press companies that publish one or more online press services recognised for political and general information (IPG). The goal is to support these press services to encourage the development of their editorial activities and ensure their economic sustainability.
- **Stakeholder benefits:** Internally, press companies benefit from financial support that helps them maintain and grow their editorial activities. Externally, readers gain access to reliable and high-quality online information, promoting a diverse and independent press landscape.
- **Accelerating mechanisms:** Key success factors include the amount of editorial expenses of the media, the number of paying subscribers, and additional financial support for newly established companies and online press services created within the last three years.
- **Link for more information:** <https://www.culture.gouv.fr/Demarches-en-ligne/Par-type-de-demarche/Subvention/Aide-au-pluralisme-des-services-de-presse-tout-en-ligne-SPTTEL>.



### PARTICIPATION

Citizens should be able to engage in the democratic process at all levels, and have control over their own data.

## Slovakia Good Practice – Brand New Code of Influencer Marketing

- **Objectives:** To promote ethical standards, transparency, and best practices in influencer marketing by providing clear guidelines for influencers, brands, and agencies, ensuring responsible collaboration and fostering trust in digital advertising (2024 – Ongoing).
- **Description:** The Brand New Code of Influencer Marketing was developed by IAB Slovakia in collaboration with the Association of Digital Marketing Agencies (ADMA). The code provides a framework for influencer marketing in Slovakia, emphasizing ethical standards, transparency, and compliance with relevant regulations. It covers areas such as disclosure of sponsored content, transparency in brand-influencer relationships, and guidelines for the responsible use of data. The goal is to ensure that influencer marketing is carried out in a way that respects both digital rights and consumer trust.
- **Stakeholder benefits:** Influencers, brands, and agencies benefit from a structured framework that enhances professionalism in influencer marketing. Consumers benefit from more transparent and ethical marketing practices, ensuring they are well-informed when engaging with influencer content.
- **Accelerating mechanisms:** Key success factors include the widespread adoption of the code by influencers, brands, and agencies, as well as continuous education and training programs. Additionally, regular monitoring and compliance checks ensure that the code's principles are upheld.
- **Link for more information:** <https://kodexinfluencermarketingu.sk/>.



### PARTICIPATION

Citizens should be able to engage in the democratic process at all levels, and have control over their own data.

## 4.4.2. Impact Indicators and Visible Results

From the six Declaration Chapters, this Chapter is among those for which relatively few statistics are available.

On the basis of the Media Pluralism Monitor a wide view can be given on *Commitment 12-15a. continuing safeguarding all fundamental rights online, notably the freedom of expression and information, including media freedom and pluralism*. In 2024, 14 out of the 27 Member States had a low risk profile in the fundamental protection area, 5 less than in 2023. These countries witness relatively low risks of violations related to freedom of expression, right to information and other media related rights.<sup>54</sup>

As far as *Commitment 12-15d. creating a digital environment where people are protected against disinformation and information manipulation and other forms of harmful content, including harassment and gender-based violence* is concerned, in 2025 60% of the EU believes that they are getting more freedom of expression and information online e.g. via online platforms, social networks and search engines. It is one of the digital rights that citizens find most protected. Nevertheless, a large part of the EU awaits further changes, as was the case in 2024 (61%) and 2023 (60%).<sup>55</sup>

Moreover, only half of the EU (53% in 2025, 53% in 2024, 52% in 2023) state that they are getting access to a trustworthy, diverse and multilingual digital environment, including more diverse content, less disinformation and less illegal content. This shows considerable and ongoing room for strengthening *Commitment 12-15e. supporting effective access to digital content reflecting the cultural and linguistic diversity in the EU*.<sup>56</sup>

No information is found on the status of the other Commitments (*Commitment 12-15b. supporting the development and best use of digital technologies to stimulate people's engagement and democratic participation*, *Commitment 12-15c. taking proportionate measures to tackle all forms of illegal content, in full respect for fundamental rights, including the right to freedom of expression and information, and without establishing any general monitoring obligations or censorship*, *Commitment 12-15f. empowering individuals to make freely given, specific choices and limiting the exploitation of vulnerabilities and biases, namely through targeted advertising*).

---

<sup>54</sup> Media Pluralism Monitor, <https://cmpf.eu.europa.eu/media-pluralism-monitor-2024/>

<sup>55</sup> Special Eurobarometer 532, 551 and 103.2 on the Digital Decade, <https://europa.eu/eurobarometer/surveys/detail/3174>

<sup>56</sup> Special Eurobarometer 532, 551 and 103.2 on the Digital Decade, <https://europa.eu/eurobarometer/surveys/detail/3174>

## 4.5. Safety, security and empowerment (Declaration Chapter V)

At the core of the EU's commitment to digital rights is the principle of ensuring safety, security, and empowerment for all users in the online space. This means designing platforms and technologies that protect individuals' privacy, give them control over their data, and empower them to navigate the digital world confidently. The story below highlights how complex privacy settings and lack of digital literacy could undermine the ability to safely engage with online services, ultimately discouraging participation.

### *Georgios*

*Georgios, a 72-year-old retired teacher, joined an online book club to connect with others and share his love for reading. However, he struggled with the platform's complex privacy settings, often unintentionally sharing personal information with others. Over time, he became frustrated and overwhelmed by the technology, feeling like he had little control over his own data. As a result, he grew hesitant to participate more actively in the book club, fearful of sharing too much information unintentionally.*

Georgios' experience underscores the importance of making digital platforms intuitive, secure, and empowering for all users, especially older individuals who may not be as familiar with the complexities of online privacy. For the digital world to be truly inclusive, it must prioritise user safety and control, providing tools that ensure individuals can confidently engage online without fear of compromising their personal information.

### 4.5.1. Implementation Initiatives

Across the EU27 Member States, 530 initiatives can be linked to **Increasing safety, security and empowerment of individuals (Chapter V)**. In particular the following Sub-chapters, Principles and Commitments are covered by the implementation efforts:

<b>Safety, security and empowerment (Chapter V)</b>	<b>530</b>
<b>A protected, safe and secure digital environment (Chapter V)</b>	<b>223</b>
<i>Principle 16. Everyone should have access to digital technologies, products and services that are by design safe, secure, and privacy-protective, resulting in a high level of confidentiality, integrity, availability and authenticity of the information processed.</i>	224
Commitment 16a. taking further measures to promote the traceability of products and make sure only products which are safe and compliant with EU legislation are offered on the Digital Single Market.	75
Commitment 16b. protecting the interests of people, businesses and public institutions against cybersecurity risks and cybercrime including data breaches and identity theft or manipulation. This includes cybersecurity requirements for connected products placed on the single market.	168

Commitment 16c. countering and holding accountable those that seek to undermine, within the EU, security online and the integrity of the digital environment or that promote violence and hatred through digital means.	157
<b>Privacy and individual control over data (Chapter V)</b>	<b>179</b>
<i>Principle 17. Everyone has the right to privacy and to the protection of their personal data. The latter right includes the control by individuals on how their personal data are used and with whom they are shared.</i>	179
<i>Principle 18. Everyone has the right to the confidentiality of their communications and the information on their electronic devices, and not to be subjected to unlawful online surveillance, unlawful pervasive tracking or interception measures.</i>	179
<i>Principle 19. Everyone should be able to determine their digital legacy, and decide what happens with their personal accounts and information that concerns them after their death.</i>	179
Commitment 17-19a. ensuring that everyone has effective control of their personal and non-personal data in line with EU data protection rules and relevant EU law.	142
Commitment 17-19b. ensuring effectively the possibility for individuals to easily move their personal and non-personal data between different digital services in line with portability rights.	37
Commitment 17-19c. effectively protecting communications from unauthorised third party access.	49
Commitment 17-19d. prohibiting unlawful identification as well as unlawful retention of activity records.	66
<b>Protection and empowerment of children and young people in the digital environment (Chapter V)</b>	<b>213</b>
<i>Principle 20. Children and young people should be empowered to make safe and informed choices and express their creativity in the digital environment.</i>	213
<i>Principle 21. Age-appropriate materials and services should improve experiences, well-being and participation of children and young people in the digital environment.</i>	213
<i>Principle 22. Specific attention should be paid to the right of children and young people to be protected from all crimes, committed via or facilitated through digital technologies.</i>	213
Commitment 20-22a. providing 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.	132
Commitment 20-22b. promoting positive experiences for children and young people in an age-appropriate and safe digital environment.	89

Commitment 20-22c. protecting all children and young people against harmful and illegal content, exploitation, manipulation and abuse online, and preventing the digital space from being used to commit or facilitate crimes.	93
Commitment 20-22d. protecting all children and young people against illegal tracking, profiling and targeting, in particular for commercial purposes.	86
Commitment 20-22e. involving children and young people in the development of digital policies that concern them.	79

Table 7. Number of initiatives related to Safety, security and empowerment (Chapter V)

When it comes to **Safety, security and empowerment (Chapter V)** the EU27 Member States have implemented a rather similar number of digital rights initiatives across the three respective Sub-chapters. Most initiatives are led by government organisations (404, compared to 86 civil society, 38 industry and 3 National Human Rights Institution initiatives). Initiatives are predominantly policy related (129), while popular measures also include training courses and educational initiatives (95) as well communication related initiatives (88). Relatively many harmonisation initiatives are also present in this area, such as guidelines and certification schemes (40). With 446 initiatives at the national level, 48 at the international level, 3 at the regional level, 34 at the local level, it is apparent that digital rights in this field are mostly promoted and protected nationally. From a historical point of view, most initiatives started in 2023, with 326 initiatives launched, followed by 2022 with 278 initiatives.

### Croatia Good Practice – Safer Internet in Pozega

- **Objectives:** Promotes digital literacy and responsible internet use among children and youth by educating students, teachers and parents through interactive workshops and school activities (2023 – Ongoing).
- **Description:** It is a local implementation of Croatia's broader effort to enhance digital safety in schools. Through a series of workshops, seminars, and hands-on activities, students learn about online threats, privacy protection, and ethical digital engagement. Schools collaborate with educators, IT professionals, and local authorities to ensure a comprehensive approach to internet safety.
- **Stakeholder benefits:** Students gain awareness and skills to navigate the internet safely and teachers receive training on integrating internet safety in the curriculum. Parents learn best practices for guiding their children's behaviour online.
- **Accelerating mechanisms:** Use of digital tools and interactive learning methods, collaborations to cyber security experts and local institutions, awareness campaigns.
- **Declaration Sub-chapters:** Protection and empowerment of children and young people in the digital environment (Chapter V).
- **Link for more information:** <https://www.skole.hr/sigurniji-na-internetu/>.



#### SAFETY AND SECURITY

The digital environment should be safe and secure. All users, from childhood to old age, should be empowered and protected.

## Estonia Good Practice - Kübertest

- **Objectives:** To assess and enhance the cybersecurity of public sector organizations, businesses, and critical infrastructure in Estonia. It aims to improve the resilience and security of digital services against cyber threats (2023 – Ongoing).
- **Description:** An initiative that offers cyber resilience testing services for Estonian organizations. By simulating real-world cyberattacks, it helps identify vulnerabilities in digital systems and offers tailored recommendations for improving security measures.
- **Stakeholder benefits:** Stakeholders, including government agencies, businesses, and IT professionals, benefit by gaining a clearer understanding of their cybersecurity posture. The initiative helps organizations to prevent cyber incidents, build trust with citizens, and ensure the continuity of critical services.
- **Accelerating mechanisms:** Collaboration with cybersecurity firms and specialists, government support, regular updates and testing and public-private collaboration.
- **Declaration Sub-chapters:** A protected, safe and secure digital environment (Chapter V).
- **Link for more information:** <https://www.kybertest.ee/>.



### SAFETY AND SECURITY

The digital environment should be **safe and secure**. All users, from childhood to old age, should be empowered and protected.

## Ireland Good Practice – National Advisory Council for Online Safety

- **Objectives:** To enhance online safety, security, and empowerment by providing expert advice, identifying emerging issues, and developing clear guidance materials for all internet users (2018 – Ongoing).
- **Description:** Established as part of Ireland's Action Plan for Online Safety, the National Advisory Council for Online Safety (NACOS) serves as a multi-stakeholder forum. It brings together experts from government, NGOs, industry, and academia to discuss and address online safety issues. The Council provides advice to the government on policy matters, identifies areas needing intervention, and develops user-friendly online safety guidance. It also reviews (inter)national research to inform its recommendations and actions.
- **Stakeholder benefits:** The government benefits from expert advice and comprehensive research that inform policy decisions. Citizens, especially vulnerable groups like children and elderly, gain access to reliable information and resources that enhance their online safety and empower them to navigate the digital world securely.
- **Accelerating mechanisms:** The success of NACOS relies on effective collaboration among diverse stakeholders, continuous monitoring of online safety trends, and the development of practical and accessible guidance materials. Regular research and feedback loops ensure the Council's recommendations remain relevant and impactful.
- **Declaration Sub-chapters:** Protection and empowerment of children and young people in the digital environment (Chapter V).
- **Link for more information:** <https://www.gov.ie/ga/foilsuichan/ebe58-national-advisory-council-for-online-safety-nacos/>.



### SAFETY AND SECURITY

The digital environment should be **safe and secure**. All users, from childhood to old age, should be empowered and protected.

## Lithuania Good Practice – Draugiškas internetas (Friendly Internet)

- **Objectives:** To create a safer and more trusted online environment for children by empowering and protecting them through various internet safety services and initiatives (2005 – Ongoing).
- **Description:** Draugiškas Internetas, part of the Lithuanian Safer Internet Centre, is an initiative aimed at promoting safer and better use of the internet and mobile technologies among children and young people. The project involves a consortium of partners, including the National Agency for Education, the Communications Regulatory Authority, Child Line, and the association "Langas į ateitį." The initiative provides a range of services, including an awareness center, a hotline for reporting illegal content, and a helpline offering psychological and emotional support. The project also organises awareness-raising events, such as Safer Internet Day, and develops educational resources for children, parents, and educators.
- **Stakeholder benefits:** Internally, the consortium partners benefit from enhanced collaboration and resource sharing, which improves the effectiveness of their internet safety efforts. Externally, children and young people gain access to reliable information and support services that help them navigate the online world safely. Parents and educators also benefit from resources and training that enable them to guide and protect children online.
- **Accelerating mechanisms:** The success of Draugiškas Internetas relies on effective collaboration among the consortium partners, continuous development of educational resources, and active participation in national and international safer internet initiatives. Regular monitoring and evaluation of the project's impact also ensure that the services remain relevant and effective.
- **Declaration Sub-chapters:** Protection and empowerment of children and young people in the digital environment (Chapter V).
- **Link for more information:** <https://www.draugiskasinternetas.lt/en/>.



### SAFETY AND SECURITY

The digital environment should be **safe and secure**. All users, from childhood to old age, should be empowered and protected.

### Italy Good Practice – Roma Digital Summit

- **Objectives:** To promote digital innovation and transformation across various sectors by bringing together key stakeholders to discuss and implement cutting-edge digital solutions (2024 – Ongoing).
- **Description:** The Roma Digital Summit, held annually in Rome, is a significant event that gathers experts, policymakers, businesses, and academia to explore the latest trends and advancements in digital technology. The 2024 edition (April 17, Palazzo Valentini) highlights generative AI, cybersecurity, and the protection of digital infrastructures. A key focus is strengthening cybersecurity resilience, protecting public digital services, and ensuring AI-driven processes are transparent and secure.
- **Stakeholder benefits:** Public administrations and businesses gain insights into secure digital transformation and compliance with cybersecurity regulations. Citizens benefit from stronger digital protections, enhanced data security, cyber resilience in public services, and increased transparency in AI-driven decision-making.
- **Accelerating mechanisms:** The success of the Roma Digital Summit relies on effective collaboration among local governments, universities, research centres, companies, and trade associations. Continuous investment in digital infrastructure, adherence to regulatory standards, and the active participation of stakeholders are crucial for achieving the summit's goals. The event provides a platform for accountability, ensuring digital rights are upheld and that investments in security strengthen both public and private sectors.
- **Declaration Sub-chapters:** Connectivity (Chapter II); Digital education, training and skills (Chapter II); Interactions with algorithms and artificial intelligence systems (Chapter III); A fair digital environment (Chapter III); A protected, safe and secure digital environment (Chapter V); Privacy and individual control over data (Chapter V).
- **Link for more information:** <https://www.theinnovationgroup.it/events/roma-digital-summit/?lang=it>.



#### SAFETY AND SECURITY

The digital environment should be safe and secure. All users, from childhood to old age, should be empowered and protected.

### 4.5.2. Impact Indicators and Visible Results

Everyone in the EU has the right to a **protected, safe and secure digital environment**. Although some key foundations seem to be in place, impact levels lay bare the need for strengthening this area too.

An example is *Commitment 16a. taking further measures to promote the traceability of products and make sure only products which are safe and compliant with EU legislation are offered on the Digital Single Market*. In 2025, 55% of the EU population feels their digital rights and principles are well applied in their country for getting access to safe and privacy-friendly digital technologies. This number sat at 55% in both 2024 and 2023 too.<sup>57</sup> In other words, almost half of the people in the EU are afraid about the safety and security risks digital technologies may bring and have the impression that no visible improvements have been made in this area.

From a duty-bearers point of view, in 2021 not even one out of five EU companies (19%) provided their employees with any training or awareness raising about the risks of cybercrime. From a rights-holders perspective, in 2020, only half of the EU citizens (49%)

<sup>57</sup> Special Eurobarometer 532, 551 and 103.2 on the Digital Decade, <https://europa.eu/eurobarometer/surveys/detail/3174>

believed that they were able to protect themselves sufficiently against cybercrime.<sup>58</sup> These figures demonstrate the necessity for ongoing actions to support *Commitment 16b. protecting the interests of people, businesses and public institutions against cybersecurity risks and cybercrime including data breaches and identity theft or manipulation. This includes cybersecurity requirements for connected products placed on the single market.*

No concrete data is available for *Commitment 16c. countering and holding accountable those that seek to undermine, within the EU, security online and the integrity of the digital environment or that promote violence and hatred through digital means.*

As far as the **privacy and individual control over data** is concerned in the EU, the status is rather similar to the cybersecurity rights, with ample room for improvement. This is illustrated with *Commitment 17-19a. ensuring that everyone has effective control of their personal and non-personal data in line with EU data protection rules and relevant EU law.* In 2023, governments declare that their raising awareness initiatives on new concepts such as personal data management based on user consent or completed for 74%, up from 66% in 2022.<sup>59</sup> Less than half of the rights-holders living in the EU (48% in 2025, 47% in 2024 and 49% in 2023) think they have proper control of their own data i.e. how it is used online and with whom it is shared.<sup>60</sup> In line with this, 67% was concerned that their online personal information is not kept secure by websites in 2020 and 60% has the same worry with public authorities.<sup>61</sup>

The same applies to *Commitment 17-19c. effectively protecting communications from unauthorised third-party access.* Half of the EU (52% in 2025, 51% in 2024 and 2023) feels their rights are recognised to get privacy online, i.e. respect for the confidentiality of communications and information on devices.<sup>62</sup> The other half fears online privacy is at stake, without substantial progress being perceived in the last three years.

A lower implementation level seems to be the case for the more specific *Commitment 17-19d. prohibiting unlawful identification as well as unlawful retention of activity records. getting control of one's digital legacy, for instance deciding what happens with personal accounts and information after one's death.*<sup>63</sup> Only four out of ten citizens of the EU population (42%) thinks this right is respected in 2025. The percentage of people that felt control of their digital legacy was similar in 2024 (41%) and 2023 (40%), for instance when deciding what happens with personal accounts and information after one's death. Digital legacy is among the least protected digital rights in the EU. The limited perceived progress compared to previous years shows a clear need to uplift the digital rights in this area.

No information was found on the impact of *Commitment 17-19b. ensuring effectively the possibility for individuals to easily move their personal and non-personal data between different digital services in line with portability rights.*

One of the ways the Declaration stimulates the **protection and empowerment of children and young people online** is with *Commitment 20-22a. providing 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.* An indication that this Commitment is not yet fully established derives from the percentage of 16 to 19 year-old

---

<sup>58</sup> <https://europa.eu/eurobarometer/surveys/detail/2249>

<sup>59</sup> Berlin Declaration Monitoring Mechanism, [https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM\\_Report\\_2023\\_vFinal\\_rev.pdf](https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf)

<sup>60</sup> Special Eurobarometer 532, 551 and 103.2 on the Digital Decade, <https://europa.eu/eurobarometer/surveys/detail/3174>

<sup>61</sup> <https://europa.eu/eurobarometer/surveys/detail/2249>

<sup>62</sup> Special Eurobarometer 532, 551 and 103.2 on the Digital Decade, <https://europa.eu/eurobarometer/surveys/detail/3174>

<sup>63</sup> Special Eurobarometer 532, 551 and 103.2 on the Digital Decade, <https://europa.eu/eurobarometer/surveys/detail/3174>

individuals with basic or above basic overall digital skills. When comparing 2023 (66%) with 2021 (69%), it becomes apparent that two thirds of the youth population have basic digital skills, but still this part is not growing.<sup>64</sup> The share of the overall population with basic digital skills has increased from 54% to 56% between 2022 and 2023.

In 2025, 42% of citizens in the EU think that the right to a safe digital environment and content for children and young people is sufficiently protected in their country.<sup>65</sup> It only partially makes up for the decline from 45% in 2023 to 39% in 2024. These findings are worrisome in light of *Commitment 20-22b. promoting positive experiences for children and young people in an age-appropriate and safe digital environment*. Given the vulnerability of children and young people, it is worrying that people perceive this area as one of the least protected digital rights from the Declaration.

The negative effects on children and youth could be severe whenever these digital rights and principles were unprotected. Moreover, the implementation status of the other related Commitments is unknown so far (*Commitment 20-22c. protecting all children and young people against harmful and illegal content, exploitation, manipulation and abuse online, and preventing the digital space from being used to commit or facilitate crimes; Commitment 20-22d. protecting all children and young people against illegal tracking, profiling and targeting, in particular for commercial purposes; Commitment 20-22e. involving children and young people in the development of digital policies that concern them*).

---

<sup>64</sup>

[https://ec.europa.eu/eurostat/databrowser/view/isoc\\_sk\\_dskl\\_i21\\_custom\\_15171872/default/table?lang=en&page=time:2023](https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i21_custom_15171872/default/table?lang=en&page=time:2023)

<sup>65</sup> Special Eurobarometer 532, 551 and 103.2 on the Digital Decade, <https://europa.eu/eurobarometer/surveys/detail/3174>

## 4.6. Sustainability (Declaration Chapter VI)

At the core of the EU's digital rights framework is a commitment to ensuring that digital devices and services contribute to sustainability and the green transition. This means developing technologies that reduce environmental impact and support a sustainable future. The story below illustrates how the digital sector must go beyond just technological advancement and design products that are energy-efficient, long-lasting, and environmentally responsible throughout their entire lifecycle.

### *Esra*

*Esra, a project manager at a tech company, was excited when her company set a goal to prioritise energy-efficient products. However, as she worked on implementing these changes, she discovered that many of the company's existing devices were not optimised for sustainability. Despite the technological advancements, the products' energy consumption and challenges with disposal revealed a significant gap in meeting true sustainability goals. She realised that the digital sector needs to design products with sustainability embedded in every stage, from production to disposal, to align with the green transition.*

These experience highlights the need for digital products and services to be developed with sustainability in mind. To support the green transition, the digital sector must prioritise eco-friendly practices across the entire lifecycle of devices, ensuring that innovation and environmental responsibility are inextricably linked.

### 4.6.1. Implementation Initiatives

Across the EU27 Member States, 145 initiatives can be linked to **Sustainability (Chapter VI)**. In particular the following Sub-chapters, Principles and Commitments are covered by the implementation efforts:

Sustainability (Chapter VI)	145
<i>Principle 23. To avoid significant harm to the environment, and to promote a circular economy, digital products and services should be designed, produced, used, repaired, recycled and disposed of in a way that mitigates their negative impact on the environment and on society and avoids premature obsolescence.</i>	145
<i>Principle 24. Everyone should have access to accurate, easy-to-understand information on the environmental impact and energy consumption of digital products and services, their reparability and lifetime, allowing them to make responsible choices.</i>	145
Commitment 23-24a. supporting the development and use of sustainable digital technologies that have minimal negative environmental and social impact.	118
Commitment 23-24b. incentivising sustainable consumer choices and business models, and fostering sustainable and responsible corporate behaviour throughout global value chains of digital products and services, including with a view to combating forced labour.	111

Commitment 23-24c. promoting the development, deployment and active use of innovative digital technologies with a positive impact on the environment and climate, in order to accelerate the green transition.	102
Commitment 23-24d. promoting sustainability standards and labels for digital products and services.	70

Table 8. Number of initiatives related to Sustainability (Chapter VI)

**Sustainability (Chapter VI)** shows relatively few initiatives compared to the other Declaration Chapters, 145 in total. In particular *Commitment 23-24d. promoting sustainability standards and labels for digital products and services* finds only 70 initiatives across the EU27. Most initiatives are led by government organisations (111, compared to 14 civil society and 20 industry initiatives). Initiatives are predominantly policy related (51) or provide research and technological solutions in this area (40). With 132 initiatives at the national level, 7 at the international level, 2 at the regional level, 4 at the local level, it is apparent that digital rights in this field are mostly promoted and protected nationally. From a historical point of view, most initiatives started in 2023, the year after the Declaration was signed, with 32 initiatives launched. The efforts of Member States in realising digital sustainability rights initiatives may also be enabled by recent EU actions, including the revised Energy Efficiency Directive (entered into force on 10 October 2023), the Ecodesign for Sustainable Products Regulation (entered into force on 18 July 2024) and Directive on Common Rules Promoting the Repair of Goods (entered into force on 30 July 2024).<sup>66</sup>

### Latvia Good Practice – Green-Tech

- **Objectives:** To promote sustainable development and the transition to a green economy in Latvia. It supports the development and implementation of green technologies that reduce environmental impact and foster innovation in industries like energy, waste management, and transportation (Ongoing).
- **Description:** An initiative that connects businesses, government agencies, and researchers to drive the development of environmentally friendly technologies in Latvia. The platform facilitates collaboration, offers resources for innovation, and provides support for green-tech startups and projects aiming to address climate change and sustainability challenges.
- **Stakeholder benefits:** Stakeholders, including businesses, government entities, and researchers, benefit by gaining access to funding opportunities, collaboration networks, and expertise in green technology development. Additionally, companies can enhance their sustainability practices, reduce their environmental footprint, and align with global environmental standards.
- **Accelerating mechanisms:** Collaboration with researchers and innovators, government incentives, networking and knowledge sharing and support for startups.
- **Link for more information:** <https://greentechlatvia.eu/en/home/>.



#### SUSTAINABILITY

Digital devices should support sustainability and the green transition. People need to know about the environmental impact and energy consumption of their devices.

<sup>66</sup> [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en)

## Romania Good Practice – Transilvania Digital Innovation Hub

- **Objectives:** Supports the digital transformation of SMEs in Romania, helping them integrate advanced technologies for improved productivity and competitiveness. A key focus is enabling businesses to adopt green technologies and sustainable practices, reducing environmental impact while advancing innovation (2017 – Ongoing).
- **Description:** The hub connects businesses with experts, technology providers, and research organizations to accelerate digital innovation. By focusing on sustainability, it offers digital solutions that help businesses lower carbon emissions, improve energy efficiency, and embrace eco-friendly practices.
- **Stakeholder benefits:** Stakeholders gain access to advanced technologies and sustainable digital solutions that improve operational efficiency and reduce environmental footprints. The hub helps SMEs align with sustainability goals while enhancing competitiveness in an increasingly green economy.
- **Accelerating mechanisms:** Access to green digital technologies, collaborative ecosystem, capacity building for sustainability, circular economy support and sustainability-focused innovation projects.
- **Link for more information:** <https://dih.transilvania.digital/>.



### SUSTAINABILITY

Digital devices should support sustainability and the green transition. People need to know about the environmental impact and energy consumption of their devices.

## Poland Good Practice – Sustainable Electro-School

- **Objectives:** Aims to educate and raise awareness about sustainable practices in the electronics sector, focusing on the responsible management of e-waste. The initiative encourages environmentally friendly behaviour in the repair, recycling, and disposal of electronic devices (2023 – Ongoing).
- **Description:** An educational project that provides training and resources on sustainable practices related to electronics. It targets students, professionals, and the general public, teaching them how to repair, recycle, and properly dispose of electronic waste to reduce environmental harm.
- **Stakeholder benefits:** Stakeholders, including students, teachers, and businesses, benefit by gaining knowledge and skills in sustainable e-waste management, promoting responsible consumption. Participants are empowered to make eco-friendly choices and contribute to the circular economy by prolonging the life of electronic devices.
- **Accelerating mechanisms:** Education and awareness, hands-on training, partnerships with industry leaders, promotion of circular economy principles.
- **Link for more information:** <https://zarazwracam.pl/zrownowazona-elektro-szkola/>.



### SUSTAINABILITY

Digital devices should support sustainability and the green transition. People need to know about the environmental impact and energy consumption of their devices.

## Portugal Good Practice - National Strategy for Smart Territories

- **Objectives:** To enhance the integration of digital technologies in rural and urban areas to foster sustainable development. It aims to improve quality of life, promote economic growth, and boost environmental sustainability through the smart use of technology (2023 – Ongoing).
- **Description:** Focuses on implementing smart technologies across Portugal to improve infrastructure, enhance public services, and create more sustainable, connected communities. The initiative leverages digital tools like IoT, data analytics, and AI to address challenges such as mobility, energy efficiency, and urban planning.
- **Stakeholder benefits:** Stakeholders, including local governments, businesses, and residents, benefit from improved infrastructure, better access to services, and increased opportunities for innovation and economic growth. The strategy promotes sustainability by enhancing resource management and reducing environmental impacts through smart technology.
- **Accelerating mechanisms:** Collaborative approach, technological integration, capacity building and training, policy and financial support.
- **Link for more information:** <https://living-in.eu/news/portugal-launches-its-first-national-smart-territories-strategy-0>.



### SUSTAINABILITY

Digital devices should support sustainability and the green transition. People need to know about the environmental impact and energy consumption of their devices.

## Germany Good Practice – Hardware for Future (*Leipzig*)

- **Objectives:** To minimize resource consumption and CO<sub>2</sub> emissions by reusing and refurbishing IT equipment, promoting digital inclusion, and ensuring sustainable digital practices (2020 – Ongoing).
- **Description:** Launched by the City of Leipzig's Digital City Unit, the "Add Hardware for Future" initiative focuses on collecting, repairing, and redistributing donated IT devices to citizens, especially low-income families. Since 2020, over 3,000 devices have been distributed, enhancing digital participation and reducing electronic waste. This effort aligns with Leipzig's Digital Agenda, which emphasizes sustainable development and digital inclusion.
- **Stakeholder benefits:** Residents gain access to affordable digital devices and support, fostering digital literacy and engagement. The environment benefits from reduced electronic waste and resource consumption, supporting sustainability goals.
- **Accelerating mechanisms:** Collaboration with volunteer associations, partnerships with public institutions, and the establishment of Wi-Fi clusters to enhance digital accessibility.
- **Link for more information:** <https://hardwareforfuture.de/>.



### SUSTAINABILITY

Digital devices should support sustainability and the green transition. People need to know about the environmental impact and energy consumption of their devices.

## 4.6.2. Impact Indicators and Visible Results

Some quantitative impact indicators are available for the sustainability related digital rights and principles. Duty-bearers related numbers cover the public sector, rather than the private sector. For instance on *Commitment 23-24a. supporting the development and use of sustainable digital technologies that have minimal negative environmental and social impact*. Public officials rate the evaluation of the energy consumption and GHG emissions resulting from ICT activities in the public sector to be completed with 74% in 2023, up from 65% in 2022.<sup>67</sup> Moreover, half of the EU citizens, 50%, believe that their country ensures digital products and services that minimise damage to the environment and society (e.g. products and services that can be repaired or recycled, and which do not involve forced labour).<sup>68</sup> The other half thinks the opposite and argues that this digital right is still at stake. The 2025 findings are similar to past observations, with 50% in 2024 and 48% in 2023.

Member States are catching up their advancements to build strategies to extend the lifespan of digital equipment used by the public sector, at a completion level of 59% in 2023, only at 38% in 2022.<sup>69</sup> Even though the private sector is not covered by this metric, these numbers indicate part of the efforts feeding into *Commitment 23-24b. incentivising sustainable consumer choices and business models, and fostering sustainable and responsible corporate behaviour throughout global value chains of digital products and services, including with a view to combating forced labour*.

Green digital rights are also still to be improved as per *Commitment 23-24c. promoting the development, deployment and active use of innovative digital technologies with a positive impact on the environment and climate, in order to accelerate the green transition*. Actions to promote the eco-design of digital public services to improve circular product cycles were considered to be completed by 64% in 2023, without major progress since 2022, 61%.<sup>70</sup>

As in the case of digital rights and principles in the online safety domain, standards can play an important role in respecting digital sustainability rights too. This is visible for instance through *Commitment 23-24d. promoting sustainability standards and labels for digital products and services*. From this perspective, actions at national or sub-national level for improving energy efficiency and optimise local consumption of digital tools and infrastructures were at a completion level of 72% in 2023, up from 65% in 2022 according to Member State representatives.<sup>71</sup> In a way, rights-holders are somewhat more reserved in their views. Around half of EU citizens is convinced that digital rights and principles are well applied in their country for getting access to the right information on the environmental impact and energy consumption of digital technologies.<sup>72</sup> Regrettably, this trust level has been slowly decreasing over time, with 49% in 2025, 50% in 2024 and 51% in 2023. Therefore, it seems that additional efforts are needed to reverse the downward trend.

---

<sup>67</sup> Berlin Declaration Monitoring Mechanism, [https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM\\_Report\\_2023\\_vFinal\\_rev.pdf](https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf)

<sup>68</sup> Special Eurobarometer 532, 551 and 103.2 on the Digital Decade, <https://europa.eu/eurobarometer/surveys/detail/3174>

<sup>69</sup> Berlin Declaration Monitoring Mechanism, [https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM\\_Report\\_2023\\_vFinal\\_rev.pdf](https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf)

<sup>70</sup> Berlin Declaration Monitoring Mechanism, [https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM\\_Report\\_2023\\_vFinal\\_rev.pdf](https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf)

<sup>71</sup> Berlin Declaration Monitoring Mechanism, [https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM\\_Report\\_2023\\_vFinal\\_rev.pdf](https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf)

<sup>72</sup> Special Eurobarometer 532, 551 and 103.2 on the Digital Decade, <https://europa.eu/eurobarometer/surveys/detail/3174>

## 5. Gaps and Challenges for Implementing and Measuring Declaration Progress

### 5.1. Awareness and Communication

In the first Study to support the monitoring of the Declaration on Digital Rights and Principles, a stakeholder survey asked respondents if they knew the Declaration. Out of 36 respondents, 26 were familiar with the Declaration (72%).<sup>73</sup> In this second study, participants were asked about this **awareness level** again. Out of 58 respondents, 46 were familiar with the Declaration (79%), particularly those representing civil (digital) rights organisations and associations. Although the sample size and technique do not allow for historical comparisons, these numbers show that the Declaration is not fully known, even though this would be desired among stakeholders who are active in the field of digital rights.

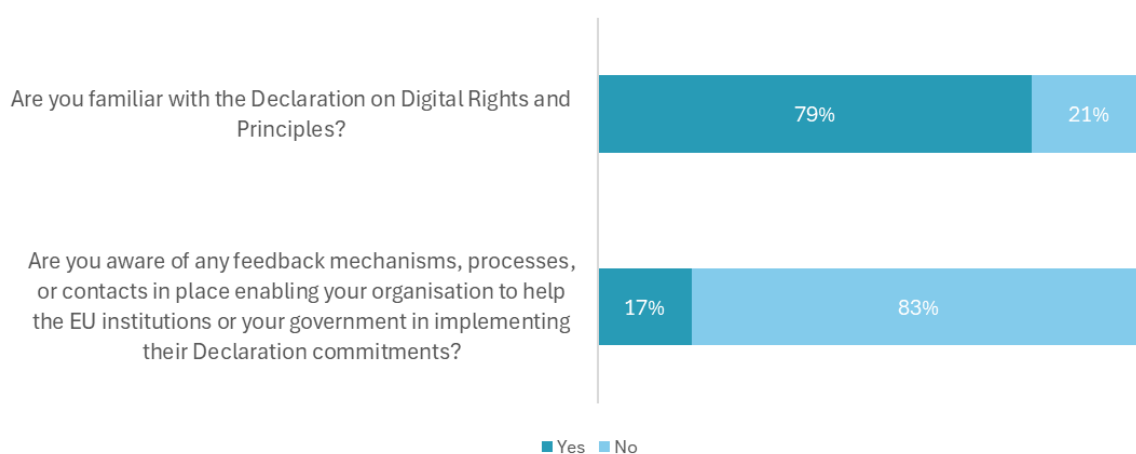


Figure 12. Awareness levels among stakeholders regarding the Declaration and feedback mechanisms

In the first monitoring study 15 persons found out about the Declaration through EU related **communication** (50%), 4 through national government communication (13%), 8 through official news sources (27%) and 3 through social media (10%). In the second monitoring study, 33 respondents got to know the Declaration through communication from the EU Institutions (51%), 6 through national government communication (9%), 9 through official news sources (14%), 14 via civil society communication (21%), and 3 through industry communication (5%).

Survey participants indicated the following possible actions to strengthen the communication towards and awareness among stakeholders with the Declaration:

- Coordinated Awareness Campaign:** stakeholders emphasize the need for a structured and widespread awareness campaign, leveraging media and communication strategies. Such as: multilingual outreach, digital engagement, and collaboration with news outlets to enhance visibility and public understanding.
- Education and Training:** survey participants highlight the importance of further integrating digital rights education into school curricula and public sector programs to ensure long-term awareness and engagement with the Declaration.
- Workshops and Stakeholder Dialogues:** respondents recommend interactive workshops and discussions involving policy makers, civil society, industry and

<sup>73</sup> <https://digital-strategy.ec.europa.eu/en/library/monitoring-digital-rights-and-principles-support-study-2024>

citizens to facilitate dialogue, engagement, share best practices and clarify the practical implications of the Declaration.

By strengthening the visibility through such communication activities, respondents believe the Declaration's implementation can become more inclusive and effective, especially when combined with efforts to formalise (new) policies and embed the Declaration's Principles and Commitments into governance structures.

## 5.2. National Feedback and Reporting Channels

In the first monitoring study, less than half of the respondents knew about feedback and reporting channels to **support the implementation of the Declaration** in their country (46%, 12 respondents). In the second monitoring study, only 10 respondents (17%) were aware of such channels. Although the survey samples are not comparable, this could be explained by the communication and promotion of these feedback and reporting channels. Member States and the EU may have emphasised the participative role of other stakeholders when the Declaration was signed at the end of 2022 but less so in recent years. As a result, fewer civil society and industry stakeholders are now familiar with these mechanisms. Examples of feedback mechanisms that were known and suggestions on how to improve them include:

- a) *Centralised Feedback Platform*: Many emphasized the need for a user-friendly, multilingual online portal where citizens can easily provide input on digital policies. This platform should be widely promoted and integrated into existing EU and national government websites.
- b) *Public Awareness Campaigns*: Respondents highlighted the importance of media outreach, social media engagement, and collaboration with news outlets to inform citizens about how they can participate. They suggested targeted campaigns, similar to GDPR awareness efforts, to make feedback mechanisms more visible.
- c) *Workshops and Stakeholder Consultations*: Many recommended organising public discussions, workshops, and interactive sessions where policymakers, civil society, industry, and citizens can share insights, exchange best practices, and better understand how feedback contributes to decision-making.
- d) *Integration into Public Services and Legislation*: To ensure lasting impact, respondents stressed that feedback mechanisms should be embedded into national policies, digital strategies, and public service processes. This would guarantee that citizen input is systematically considered in digital policy development.

By improving these areas, respondents believe the Declaration's implementation can become more accessible, transparent, and effective in shaping digital policies.

## 5.3. Future Priorities

In terms of a 2025 and onwards outlook, additional digital rights initiatives can be expected. Stakeholder survey respondents indicated their priorities for the next 12 months, providing an indication on how European organisations plan to stimulate digital rights and principles in different areas. When looking at the **stakeholder priorities**, it becomes clear that civil society and industry stakeholders indicated to prioritise especially Declaration Chapter I for the next 12 months. Based on the same second monitoring study survey, Declaration Chapter VI was least mentioned to be a top or high priority.

Whenever these findings would be representative to the full range of organisations working on digital rights and principles, it seems that those Declaration Chapters for which already most initiatives have been put in place, are also the Declaration Chapters for which most new initiatives are to be expected.

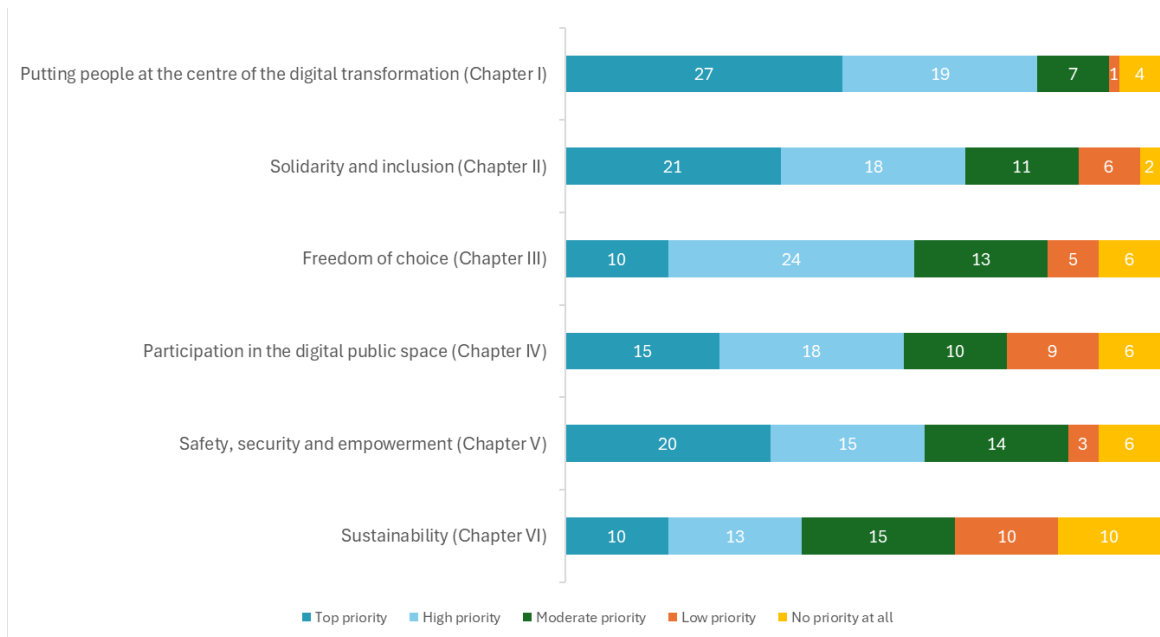


Figure 13. The number of surveyed stakeholders that plan to prioritise initiatives for each of the Declaration Chapters in 2025

Concrete examples of future initiatives and actions include, mentioned by stakeholders:

- Digital Rights Playing Cards:** An organisation is designing interactive playing cards focused on Digital Rights and Principles. These cards will be used in workshops and integrated into their website, offering a “daily digital right” feature on request.
- Local Digital Rights Pilots:** A growing number of organisations (government and business organisations) that develop pilot projects that enable cities to implement participatory democratic mechanisms such as citizen assemblies, open forums, platforms for public discourse and debates.
- Digital Inclusion:** More support is being provided for senior citizens/employees to improve their digital skills (government, civil rights, and business organisations). A few organisations stated that this includes public talk, training programs, and accessible digital education initiatives to enhance the digital skills and bridge the digital divide.
- Research Projects:** Several organisations recognised the need to strengthen their commitment to the Declaration by increasing its reference in official publications, such as reports and advisory opinions. Additionally, they emphasized the importance of ongoing monitoring and promotional activities to enhance awareness and implementation.
- Artificial Intelligence:** A growing focus is being placed on AI governance and its use by municipalities. Organisations are pushing for more discussions on AI ethics, transparency, and accountability at the local government level.

## 5.4. Implementation and Data Gaps

Which digital rights areas are most at risk? This could be due to limited implementation initiatives, limited quantitative impact indicators or low quantitative impact levels for measured areas. What implementation and data availability gaps need to be addressed?

**Implementation efforts** are mostly seen in the area of *Solidarity and inclusion (Chapter II)* and *Safety, security and empowerment (Chapter V)*, followed by *Putting people at the centre of the digital transformation (Chapter I)*. *Freedom of choice (Chapter III)* and

*Participation in the digital public space (Chapter IV)* have fewer initiatives. *Sustainability (Chapter VI)* is supported by the lowest number of digital rights initiatives. When looking at the Declaration's Sub-chapters it becomes clear that governments, National Human Rights Institutions, civil society and industry have launched most initiatives in the areas of *Digital education, training and skills (Chapter II)*, as well as *A protected, safe and secure digital environment (Chapter V)*. Conversely, biggest gaps persist in the areas of *A fair digital environment (Chapter III)* and *Fair and just working conditions (Chapter II)*. These areas affect the digital rights of consumers and employees in the EU. Historically, the distribution of digital rights initiatives across the six Declaration Chapters has remained stable. In other words, areas with many actions continue to see most new initiatives. The opposite is also true. Areas with fewer actions see fewer new digital rights initiatives.

**Data availability** for monitoring impact levels varies across the digital rights. All Commitments in Declaration Chapter *Sustainability (Chapter VI)* can be tracked with quantitative impact indicators. A majority of Commitments can be monitored too for *Putting people at the centre of the digital transformation (Chapter I)*, *Solidarity and inclusion (Chapter II)*, *Freedom of choice (Chapter III)* and *A protected, safe and secure digital environment (Chapter V)*. However, less than half of the Commitments in Declaration Chapter *Participation in the digital public space (Chapter IV)* are backed up by quantitative monitoring data. The study seeks to provide relevant quantitative data where possible. The challenge of limited data availability is evident across multiple digital rights areas. In particular, quantitative impact data is not yet fully available for the areas of *Fair and just working conditions (Chapter II)* and *Protection and empowerment of children and young people in the digital environment (Chapter V)*. For instance, it is unknown to what extent Member States respect *Commitment 5-6b. ensuring that, in the working environment, digital tools do not put workers' physical and mental health at risk in any way*, and *Commitment 20-22c. protecting all children and young people against harmful and illegal content, exploitation, manipulation and abuse online, and preventing the digital space from being used to commit or facilitate crimes*.

When examining the quantitative impact indicators, most **impact and visible results** of digital rights initiatives are found in the area of *Putting people at the centre of the digital transformation (Chapter I)* and *Solidarity and inclusion (Chapter II)*, followed by *Freedom of choice (Chapter III)* and *Sustainability (Chapter VI)*. The areas of *Participation in the digital public space (Chapter IV)* and *Safety, security and empowerment (Chapter V)* show lower impact scores. These areas do not seem to demonstrate strong protection of digital rights yet. This is remarkable for *Safety, security and empowerment (Chapter V)*, given the relatively high number of digital rights initiatives in the security and safety space. In general, indicators show that duty-bearers (e.g. governments) have more optimistic stances towards the impact of digital rights initiatives than how they are perceived by rights-holders (e.g. citizens, consumers, employees and others living in the EU).

In sum, the **implementation and data gaps** seem most pressing in the area of *Participation in the digital public space (Chapter IV)*. There are fewer digital rights initiatives in this area, fewer statistical data sources are available, and both duty-bearers and rights-holders perceive the impact of existing digital rights initiatives for the Commitments made by Member States as mediocre. Stakeholders appear to prioritise other digital rights and principles more urgently than ensuring a trustworthy and diverse digital environment, with the right to free expression and information, transparency of media ownership or support for a democratic debate by online platforms.

## 6. Conclusions and Recommendations

This study analysed **2,177 digital rights initiatives** relevant to the six Declaration Chapters, implemented across EU27 Member States. The digital rights initiatives are predominantly associated with two main Declaration areas: *Solidarity and inclusion (Chapter II)* and *Safety, security and empowerment (Chapter V)*. Efforts specifically focus on improving *Digital education, training and skills (Chapter II)*, as well as ensuring *A protected, safe and secure digital environment (Chapter V)*. Digital rights initiatives have also actively contributed to overarching Commitments of *Putting people at the centre of the digital transformation (Chapter I)*. Fewer digital rights initiatives were found for *Freedom of choice (Chapter III)*, *Participation in the digital public space (Chapter IV)* and in particular *Sustainability (Chapter VI)*. The total number of digital rights initiatives has been steadily growing over the years. At the same time, it should be noted that the number of newly launched digital rights initiatives has been slowing down after 2023.

The study provides relevant quantitative data where possible. For two-thirds of the Declaration Commitments statistical sources can estimate their impact. The impact of the remaining Commitments has been difficult to quantify so far, partly due to lack of available data both from the perspective of duty-bearers as well as rights-holders. When examining these quantitative impact indicators, most **impact and visible results** are found in the area of *Putting people at the centre of the digital transformation (Chapter I)* and *Solidarity and inclusion (Chapter II)*. In contrast, *Participation in the digital public space (Chapter IV)* and *Safety, security and empowerment (Chapter V)* do not yet seem to show such protection of digital rights, despite Member States' efforts in the security and safety space relevant to the fifth Chapter.

Based on these observations, the study brings forward the following key **recommendations**.

1. Member States may increase the **Declaration's visibility** and highlight its overall importance. Digital rights covered by existing initiatives should be strengthened and should not fade away, for instance those related to *Solidarity and inclusion (Chapter II)* and *Safety, security and empowerment (Chapter V)*. Although the total number of active digital rights initiatives has grown over time, the number of new initiatives has slowed after 2023. Fostering new initiatives is needed to support currently overlooked areas. Additional Member States' efforts on the Commitments related to *Participation in the digital public space (Chapter IV)* and *Sustainability (Chapter VI)* are necessary based on current monitoring findings. In the spirit of the Declaration, efforts may become more effective and efficient if relevant stakeholders work together. Existing government initiatives could be advanced by National Human Rights Institutions, civil society and industry. Similarly, national initiatives can be expanded into international initiatives, as well as regional and local initiatives, to maximise impact.
2. The European Commission should coordinate the work in order to improve the data availability for monitoring the Declaration's progress based on **a more comprehensive set of quantitative impact indicators**, for which annually collected data is available. Alternative or new data sources should be considered for the 17 Commitments on which no monitoring data is available. As noted, the need for comparative EU27 indicators is most apparent in the area of *Participation in the digital public space (Chapter IV)*. A possible way to go about the development of new indicators would be to pilot such indicators in a selection of Member States. This may require aligning on recent data collection initiatives from individual Member States, such as: the Spanish Digital Rights Observatory that holistically addresses and oversees digital rights<sup>74</sup>, the German

---

<sup>74</sup> <https://www.derechosdigitales.gob.es/>

Government Report on Older People<sup>75</sup> and the Danish Trust in Digital Government Survey relevant to *Solidarity and inclusion (Chapter II)*<sup>76</sup>, the Slovakian Hate Speech on Social Media Study linked to *Participation in the digital public space (Chapter IV)*<sup>77</sup> and the Digital Barometer in Finland with relevance to *Freedom of choice (Chapter III)*.<sup>78</sup> The European Commission may also liaise on different data sources with other institutions, such as: the European Union Agency for Fundamental Rights and its Data Dashboards<sup>79</sup>, digital rights reports from the Council of Europe<sup>80</sup>, European Network of National Human Rights Institutions monitoring good practices<sup>81</sup>, and United Nations digital space initiative.<sup>82</sup> In any case, the measurement burden on Member States should be minimised as much as possible when introducing new indicators.

Replacement indicators should be identified for those derived from the **Berlin Declaration Monitoring Mechanism**. This annual measurement published its final data in 2024, covering 2021, 2022 and 2023. It is not expected to continue. This affects the monitoring of 15 Commitments, part of *Putting people at the centre of the digital transformation (Chapter I)*, *Solidarity and inclusion (Chapter II)*, *Freedom of choice (Chapter III)*, *Safety, security and empowerment (Chapter V)* and *Sustainability (Chapter VI)*. Currently, the number of indicators reflecting duty-bearers' and rights-holders' perspectives is balanced. The Berlin Declaration Monitoring Mechanism provides insight into the impact of duty-bearers. Replacement indicators should keep this balance.

For indicators reflecting the views of rights-holders, a potential improvement would be to extend the **Special Eurobarometer on the Digital Decade** and include survey items for all Commitments or at least cover all areas of the Declaration (all Sub-chapters). As it currently stands, the Special Eurobarometer on the Digital Decade covers eleven out of thirteen Sub-chapters. Adding a survey question for *Solidarity and inclusion (Chapter II)* and *A fair digital environment (Chapter III)*, would enhance the coverage and relevance of the measurement. For instance, a related Commitment that yet lacks quantitative impact data and could be prioritised is *Commitment 2c. developing 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 infrastructures, for the benefit of all people living in the EU*. This would promote greater validity of the Special Eurobarometer on the Digital Decade. The revision of the Digital Decade Targets in 2026 may also provide momentum and relevant discussions to achieve this.

To enhance the monitoring of the Declaration, **data collection and publication timelines** may need to be realigned. Both the first and second support study to the monitoring of the Declaration were published along the State of the Digital Decade Report halfway the year. However, most underlying data sources are published in the second half of the year, with data collection occurring the year before. Consequently, several indicators in this 2025 report cover data from 2023, while 2024 or even 2025 data become available shortly after publishing the State of the Digital Decade Report. In general data sources with annual data collection should be prioritised, to allow for year-to-year comparisons. While some sources are only available biennially or less frequently, annual data improves comparability and consistency between indicators over time.

<sup>75</sup> <https://www.bmfsfj.de/resource/blob/159708/ed36ad230d6038b9f0a439fb03ddf35b/achter-altersbericht-kurzfassung-englisch-data.pdf>

<sup>76</sup> <https://en.digst.dk/digital-transformation/trust-in-digital-government/#accordion-digital-inclusion>

<sup>77</sup> <https://www.snsjp.sk/aktuality/ake-formy-nenavistnych-prejavov-sa-vyskytuju-na-socialnych-sietach/>

<sup>78</sup> <https://www.etla.fi/digibarometri/>

<sup>79</sup> <https://fra.europa.eu/en/databases/efris/data-dashboards>

<sup>80</sup> <https://www.coe.int/en/web/portal/council-of-europe-and-internet>

<sup>81</sup> <https://ennhri.org/ai-resource/good-practices/#monitoring>

<sup>82</sup> <https://www.ohchr.org/en/topic/digital-space-and-human-rights>

## Annexes

### I. Country Factsheets

Attached to this report are country factsheets, with specific key numbers for each of the EU27 Member States. These factsheets are included in the 2025 Digital Decade Country Reports.

### II. Data File (Excel)

[The data file](#), including the findings of the desk research and quantitative impact indicators<sup>83</sup>.

---

<sup>83</sup> Data File (Excel) is available here: <https://digital-strategy.ec.europa.eu/en/news-redirect/116804>

## GETTING IN TOUCH WITH THE EU

### In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)

### On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696, or
- by email via: [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)

## FINDING INFORMATION ABOUT THE EU

### Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: [https://europa.eu/european-union/index\\_en](https://europa.eu/european-union/index_en)

### EU publications

You can download or order free and priced EU publications from: <https://op.europa.eu/en/publications>. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)).

### EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: <http://eur-lex.europa.eu>

### Open data from the EU

The EU Open Data Portal (<http://data.europa.eu/euodp/en>) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

