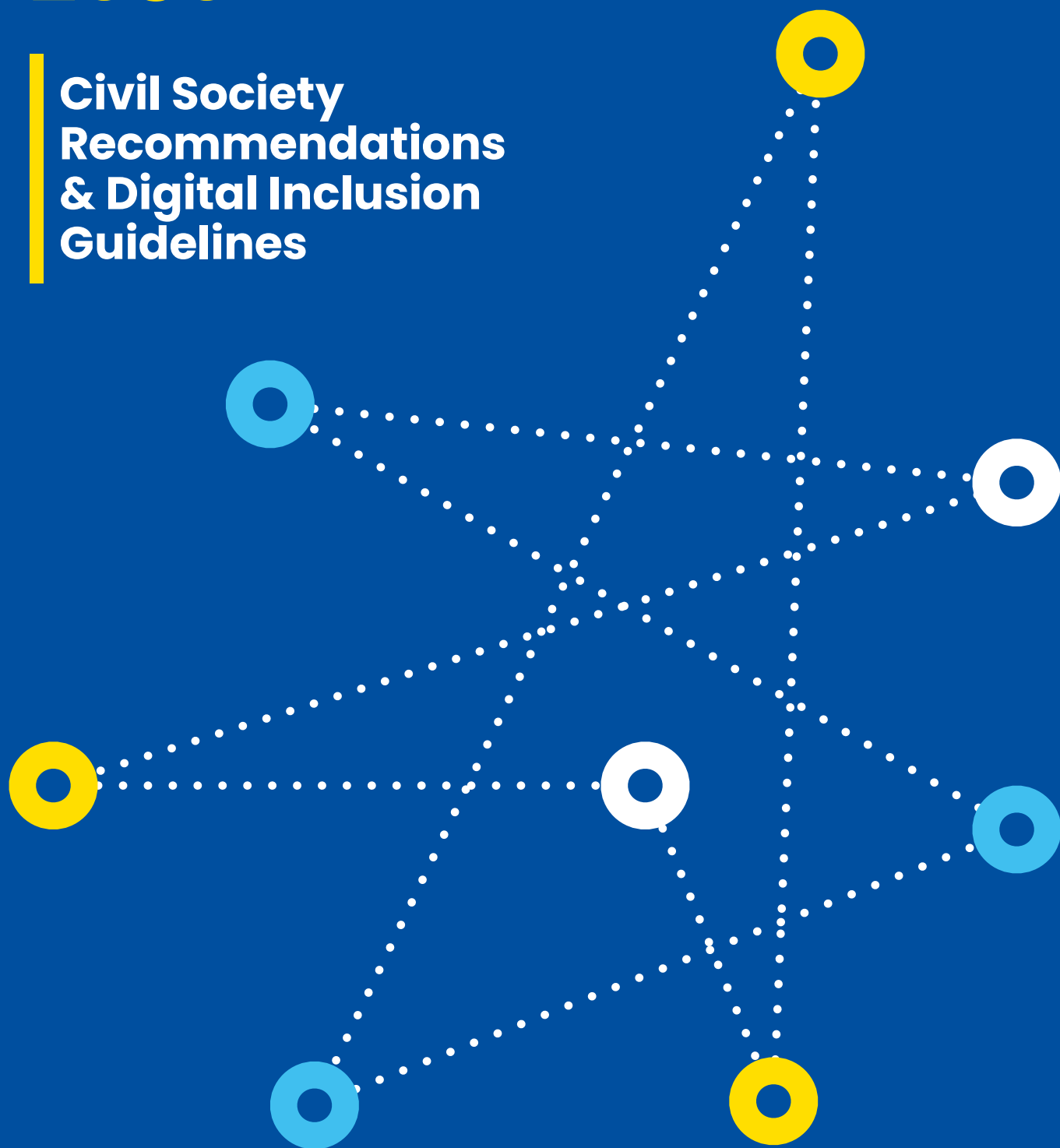


The EU's Digital Transformation 2030

Civil Society
Recommendations
& Digital Inclusion
Guidelines



Co-funded by
the European Union



ECAS Brussels, April 2024

ELISA LIRONI

Programme Director – European Democracy, ECAS

SILVIA DEMOFONTI

Accessibility and Equity Manager, ECAS



Co-funded by
the European Union

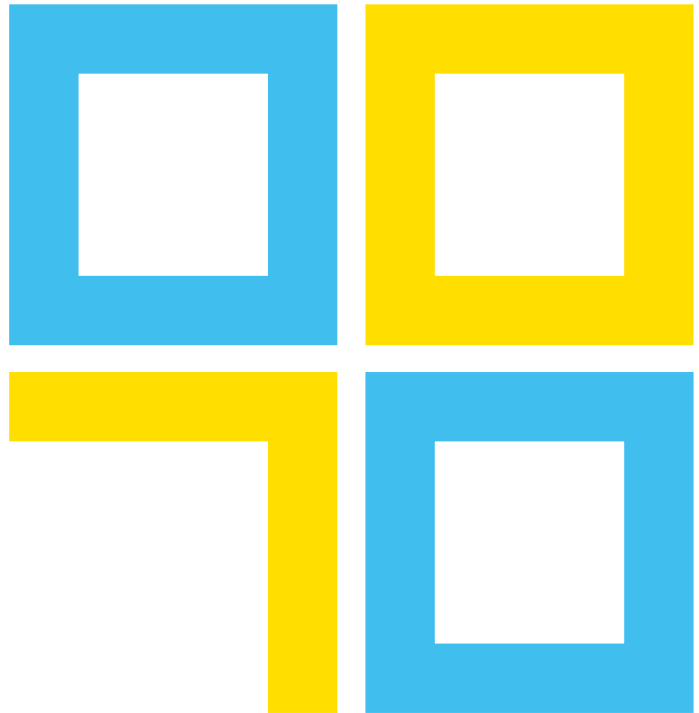
“Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.”

Content

1. INTRODUCTION	03
2. CIVIL SOCIETY RECOMMENDATIONS ON DIGITAL TRANSFORMATION	05
2.1. Digital Democracy	09
Recommendations	10
2.2. Digital Economy	13
Recommendations	14
2.3. Digital Rights and Freedom	18
Recommendations	19
2.4. Digital Safeguards	22
Recommendations	23
2.5. Digital Education	28
Recommendations	29
3. DIGITAL INCLUSION GUIDELINES	32
3.1. Infrastructure requirements: Resources, Security and Design	34
3.2. Supporting ecosystem: Assistive services, Education initiatives, Communication campaigns	38

1.

Introduction



As technology continues to constitute turning points in modern history, affecting the way we live, work and evolve, Europe has important decisions to take in shaping its digital future and strengthening its capacities in new technologies. Although digital policies have been one of the cornerstones of EU legislation since many years, the main and most important challenge today is to achieve a digital transformation that works for all, without further deepening the existing digital divide or creating new inequalities. Civil society organisations in Europe are raising concerns regarding privacy issues, the surveillance of people, racism in Artificial Intelligence and algorithms, and biometric mass surveillance technologies, as well as lack of accessibility of new technologies. It is crucial to put human rights first and allow for a digital transformation in Europe that is shaped by the people for the people.

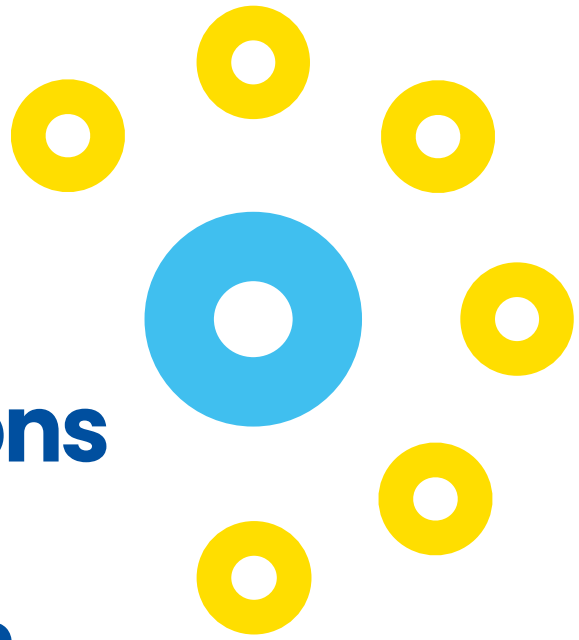
The first part of this report presents **a set of policy recommendations from European civil society organisations that can support policymakers in ensuring an inclusive EU Digital Transformation process**. In 2021, ECAS joined the Civil Society Convention on the Future of Europe, a network of more than 80 organisations

all over Europe. The Convention was structured around 5 thematic clusters and actively engaged in observing the democratic functioning of the Conference on the Future of Europe (CoFoE) and ensuring genuine involvement of NGOs in this process. In this context, ECAS's Programme Director for European Democracy, Elisa Lironi, chaired the Digital Transformation cluster, which aimed at bringing proposals of civil society organisations that could feed into the EU's priority of "A Europe fit for the digital age". The ambition of this priority was to strengthen the EU's digital sovereignty and set standards on data, technology, and infrastructure – with a clear focus on education, ethics, fundamental rights and European values. To achieve that, the cluster implemented an intense crowdsourcing process receiving recommendations from Civil Society Organisations across Europe on how to ensure inclusive policies in five broad Digital Transformation categories: **Digital Democracy, Digital Economy, Digital Education, Digital Safeguards and Digital Rights**. This crowdsourcing exercise received 216 ideas and recommendations from about 1200 CSOs across Europe. These ideas were discussed and elaborated in 84 recommendations published in Chapter 5 of the Civil Society State of the Union Report 2023 in September 2023, thanks to the consultations with many European CSOs coordinated by the organisation Civil Society Europe. In 2023, ECAS worked together with civil society organisations and Civil Society Europe to have an updated version of CSOs' recommendations on how the EU should proceed with its digital transformation policies.

In the second part, the report presents the final **Digital Inclusion Guidelines**, which are the result of comparative analyses between the contributions received from the different Member States on the civil society recommendations. ECAS held, together with local organisations, co-creation events in five different Member States in 2022: Ireland, Portugal, Latvia, Belgium and Luxemburg; and five events in five Member States in 2023: Germany, Greece, Croatia, Italy and Bulgaria. During the events, ECAS presented the main challenges of digital transformation towards inclusion at the EU level and showcased the recommendations advocated by civil society organisations across Europe. The participants then proposed their own recommendations and ensured that citizens' interests, and mainly the interests of vulnerable groups, are included in the development of the EU's ongoing and future Digital Transformation strategy. The results from all these events were analysed and developed into the Digital Inclusion Guidelines, whose function is to serve as a guide for policymakers striving to safeguard the interests of vulnerable and diverse groups in the process of Digital Transformation in the EU.

2.

Civil society recommendations on digital transformation



The proposals developed under the Digital Transformation Working Group, initially for the Civil Society Convention on the Future of Europe in 2021-2022 and subsequently for Civil Society Europe in 2023, aim to feed into the European Commission's priority of 'A Europe fit for the digital age' and its targets until 2030. The ambition of this priority has been to strengthen the EU's digital sovereignty and set standards on data, technology, and infrastructure – with a clear focus on education, ethics, accessibility, fundamental rights and European values.

Since 9 May 2022, the last day of the Conference on the Future of Europe (CoFoE), the EU has moved forward in the adoption of several key legislations CSOs have been monitoring closely and striving for: the Digital Markets Act (DMA), the Digital Services Act (DSA), the revised Audiovisual Media Services Directive (AVMSD) and even the regulation on Markets in Crypto-Assets (MiCA). These are fundamental steps to prevent large online platforms from abusing their market power; to address problematic aspects of online services, such as the lack of accountability, low transparency, and how online discourses are shaped; to recognise the importance of

media services of general interest and increase the accessibility to these services; and to regulate and establish a harmonized set of rules for crypto-assets.

CSOs have also been calling for working conditions for online platform workers to be better regulated at the European level in order to address new forms of precariousness, insufficient social protection and the issue of algorithmic management. To this aim, the EU has also been working on a new Platform Workers Directive, whose objective is to improve the conditions of people working through digital platforms while preserving the opportunities and benefits brought by the platform economy. CSOs will ensure that uniform operation rules, open competitiveness and common principles on workers' conditions will be at the heart of this new directive.

While the adoption of these digital policies have answered to several of CSOs's key demands, there is still a long way to go in order to ensure a digital transformation in Europe that leaves no one behind. In 2023, the Digital Transformation Working Group has continued its focus on five main topics to develop updated recommendations on: digital democracy, digital education, digital safeguards, digital rights and freedoms, and the digital economy.

Digitalisation is becoming ever more ubiquitous and, indeed, is now a necessity in everyday life. On the one hand, EU citizens are constantly part of digital democracy by using online public services, receiving important information through the Internet and often having the opportunity to engage in democratic life through e-participation channels. Over the last decade, the EU has focused its e-government and e-transparency efforts on technological solutions for public administrations, businesses and people (e.g. electronic identity). For e-participation, a few channels currently play an important role in citizen engagement, such as the European Citizens' Initiative. However, these channels are not sufficient for the meaningful involvement of EU citizens and e-participation tools need to be more inclusive, used in a structured way, accessible for everyone and, in particular, more impactful.

On the other hand, citizens are also now part of a society focused more and more on

the digital economy, which refers to the development of an economy that is based on digital computing technologies. The economy is changing, and digital business models are amongst the most profitable having impacted the entire EU, bringing both opportunities and challenges. A successful digital strategy is one that takes advantage of opportunities by creating benefits for the entire society whilst appropriately addressing the challenges.

Technology constantly has an impact on how European citizens conduct their daily lives, the EU has important decisions to take in shaping its digital future and strengthening its capacities in new technologies. In 2021, the European Commission presented a vision and avenues for the EU's digital transformation by 2030 in its Digital Compass for the EU's digital decade, which evolves around four cardinal points: government, skills, infrastructures, and businesses. Although the EU has set ambitious targets, frameworks and projects to ensure its digital development, civil society organisations have raised concerns about the impact of current and future European policies and measures on citizens and the environment.

The main and most important challenge is to achieve a digital transformation that works for all, without further deepening the existing digital divide or creating new inequalities. For the EU to be a front runner in the digital domain, EU institutions and Member States must ensure that all citizens have access to basic digital technologies and are provided with the right skills to navigate the digital world. A digital transformation that is truly inclusive means tackling the inequalities that exist across the Union by enabling and facilitating online access, especially to parts of our society at risk of marginalisation – persons with disabilities, seniors, migrants, homeless people, people at risk of poverty and social exclusion, women and many more. For this reason, EU institutions and Member States should make access to affordable, high-speed Internet a fundamental right for their citizens. If Internet access is both guaranteed and accessible, digital education will become a priority and evenly implemented across all Member States to equip people with the right skills and competencies, resulting in greater citizen involvement, especially in the EU's digital democracy and digital economy.

Digitalisation will only advance European societies if we can safeguard and strengthen

our democracies in the process. To this end, several digital policies are still needed at the EU level to ensure that the digital technologies developed and used respect human rights and democratic principles. Especially in 2023, various EU legislative processes have already put in place safeguards to human rights while stimulating innovation and market integration (such as the AI Act, the DSA, the DMA, etc.). There is great potential for the EU to be an ambitious rights-driven leader in tech policy, but this will only be possible if it places human rights and democratic principles at the centre of these legislative processes, alongside innovation and competition concerns. For example, AI respecting fundamental rights must be allowed to develop in the EU, or it will be developed in other parts of the world with far fewer safeguards.

In conclusion, European digital policies are a mixed bag of good policies and policies that need to enhance the protection of citizens' rights and online freedom. Platform regulations are going in the right direction and could start bringing power to the people rather than to 'big tech'. However, the EU's effort is simply not enough. As already mentioned, civil society organisations are raising concerns regarding several issues that have yet to be solved, including privacy issues, the use of biometric mass surveillance technologies, racism in AI and algorithms, as well as the lack of access to new technologies. The EU needs to focus on putting human rights first and enabling a digital transformation that is shaped by the people for the people..

The civil society recommendations on **digital democracy, digital economy, defending rights and freedom online, digital safeguards and digital education** are presented in the following subchapters.

2.1

Digital Democracy

The use of Information and Communication Technology (ICT) in political and governance processes should be increased in an efficient and accessible manner to allow more services and interaction between citizens and their governments. Different aspects of digital democracy include:



1. E-GOVERNMENT:

The use of ICT to enhance public administration or public services.



2. E-TRANSPARENCY:

The use of ICT to enhance transparency of governments by allowing citizens to access information online.



3. E-PARTICIPATION:

The use of ICT to allow citizens to participate in decision making processes, to improve policy outputs, and even co-create politics together with their representatives.



4. E-VOTING / E-ELECTIONS:

To allow voters to record secret ballot and have it tabulated electronically in an election system.

MAIN CHALLENGES:



ENSURE ACCESSIBILITY



ENSURE INCLUSIVENESS



ENSURE TRANSPARENCY

RECOMMENDATIONS:

E-PARTICIPATION

- EU institutions and national governments should actively promote and clearly communicate e-participation in decision-making and **provide citizens with a realistic opportunity to impact policy-making and legislative processes.**
- **European citizens' capacity to engage in e-participation** should be strengthened, as well as the impact their contributions make in policymaking. They should always receive feedback to what extent their inputs to decision-making are taken into account and why (or why not).
- E-participation mechanisms and channels should be extended by **testing and combining new methods of citizen engagement** at the EU level, e.g. crowdsourcing legislation and participatory budgeting.
- The EU should focus on the next legislative term on ensuring the enforcement of existing digital horizontal policies.
- EU Member States and the European Parliament should proactively explore opportunities as well as address the legal, technical and societal challenges of **e-voting/e-elections** by promoting voting pilots and test beds on the Internet.
- The EU should **pilot e-voting** at the next European elections, provided it is **technically secure, efficient and can guarantee transparency in the process.**
- EU Institutions and Member States should **ensure accessibility of digital means (secure and quality Internet connection) to citizens everywhere**, in order to shorten the digital divide and allow for equal access to e-voting and online participation across the EU.

E-GOVERNMENT

- The EU should make **access to free, equal and affordable Internet as a fundamental right** of every EU citizen - given the importance today of having

access to the Internet for a significant number of vital tasks, access to the Internet should be guaranteed for everyone. In this respect, specific EU- and nationally funded programmes could be allocated for vulnerable groups and people at risk of poverty or social exclusion to ensure they can afford to use the Internet.

- E-government solutions should be developed in **consultation with the end-users and civil society organisations** to ensure solutions are **accessible and inclusive** for everyone, efficient, trustworthy, safe, subject to privacy and controlled by humans.
- **Alternatives to e-government services** must be provided to ensure that those who do not have the possibility to use digital tools, and persons with disabilities or with low digital literacy can still be adequately engaged and served appropriately.
- E-government public data and documents at the national, regional and local level should be **accessible, according to the Web Accessibility Directive, and usable in open formats**, and the content should be user-friendly, both in terms of the language used and its location.
- **Provide public services that are fully accessible** for hard-to-reach segments of the population, by: a) **funding and collaborating with civil society organisations** which currently support those who are excluded from the digital transition; b) **expanding initiatives that support and guide citizens in the digital transition** (such as France's 'conseillers numériques') adapting them if needed and learning from both their failures and successes.
- Ensure that publicly financed software developed for public sector e-government solutions is made available under **a free and open-source software licence**.
- **Ensure safe, secure and privacy-respecting national electronic identification schemes across borders** in order to create an effective European Digital Identity (eID) that enables safe and easy access to digital public services and online tools.
- EU institutions and Member States should encourage and leverage “the transformative, innovative and collaborative power of open source, its principles and development practices” in e-government. They should also promote the

sharing and reuse of software solutions, knowledge and expertise to deliver better e-government services that benefit society and lower society's costs.

E-TRANSPARENCY

- To ensure e-transparency that leaves no citizen behind, **information must be easy to understand, easy to find, and accessible for everyone**. This includes providing information in national sign languages and an easy-to-read format. The platforms, tools and technologies required to access this information should also be accessible. Furthermore, citizens must always be given the option of non-digital access to information.

2.2 Digital Economy

The development of an economy that based on digital computing technologies that is fully respectful of the environment and benefits society as a whole. It includes concepts such as:

1. DIGITAL INDUSTRY 5.0

(e.g. Internet of Things, Cloud Computing, etc.):

Industry 5.0 is the comprehensive transformation of the whole sphere of industrial production through the merging of digital technology and the Internet with conventional industry.

2. DIGITAL FINANCE:

The impact of new technologies on the financial services industry. It includes a variety of products, applications, processes and business models that have transformed the traditional way of providing banking and financial services.

3. DATA ECONOMY:

The creation of a single market for data in the EU where data can flow across sectors to benefit all and the rules for access and use of data are fair, practical, clear and respected.

4. SUPPORTING GREEN DIGITAL SOLUTIONS:

The use of green digital technologies for the benefit of the environment - mainly by developing and investing more green digital technologies to achieve climate neutrality and accelerate the green and digital transitions in priority sectors in Europe.



5. SOCIAL WELFARE IN THE DIGITAL AGE:

Digital transformation of public welfare services.



6. DIGITAL BUSINESS / COMPANIES:

The use of technology to create new value in business models, customer experiences and the internal capabilities that support its core operations (e.g. Uber, Amazon, etc.).

MAIN CHALLENGES:



ENSURE ACCESSIBILITY



CREATION OF SINGLE MARKET FOR DATA IN THE EU

RECOMMENDATIONS:

DIGITAL ECONOMY, DIGITAL FINANCE AND DATA

- For a thriving digital economy, **digitalisation should be inclusive and participatory** so that nobody is left behind due to inaccessibility, unavailability, unaffordability of technologies for citizens, or due to their lack of connectivity or digital skills.
- In this regard, **essential services provided by private actors, like banking, should be accessible offline** to ensure people who may be digitally excluded (the elderly, those without appropriate skills, those facing material deprivation, etc.) continue to enjoy access to these services.
- Since more and more services are available online and data is stored and processed by private companies and public institutions, **strong safeguards for very sensitive data** (such as migration status, health records, or receipt of welfare benefits) must be put in place for the European Single Digital Market for

Data.

- The EU should ensure **fair taxation of the digital economy across all Member States**.
- Moreover, it should **introduce corporate tax rules** so that profits are registered and taxed based on where geographically businesses have significant interaction with users through digital channels.

SOCIAL WELFARE IN THE DIGITAL AGE

- EU institutions and Member States need to **support digitally and socially excluded groups** with funds, resources and digital transition programmes. These should be specifically targeted at people left behind due to inaccessibility, unavailability, or unaffordability of technologies, or due to their lack of connectivity or digital skills.
- **Welfare benefits** aimed at alleviating poverty or social exclusion, such as minimum income schemes, **should be accessed by online and offline channels**. Digital and social exclusions are often intertwined, therefore digital-by-default options for accessing these benefits may be an unjustified barrier.

SUPPORTING GREEN DIGITAL SOLUTIONS

- **Sustainability and energy efficiency** have to be ensured at the level of the production of digital devices, as resources needed are still mined under socially and environmentally disastrous conditions. Furthermore, products should come with **information on energy consumption** in their production process. There must be a focus on durability and possibilities for repair and reuse.
- Similar **sustainability considerations must accompany the provisioning of digital services and Internet governance**, which is especially important given the popularity of streaming services and the considerable amount of energy going into the training and serving of AI systems.
- The EU must ensure **comprehensive and transparent assessments** by conducting thorough studies that **consider the end-to-end life cycles**

and supply chain emissions of ICT, with a focus on accurate estimates, interrogability, and disclosure of potential conflicts of interest (resources needed are still mined under socially and environmentally disastrous conditions; products should come with information on energy consumption in their production process).

- The EU should also **embrace digital sobriety principles**: prioritise sustainable practices within the ICT sector, such as promoting energy efficiency, minimizing data storage (especially for what concerns videos) adopting responsible digital preservation techniques, encouraging best daily practices for reducing the use of energy, utilizing renewable energy sources, and emphasizing repair and reuse - especially concerning devices.
- It is crucial to **set science-based net-zero targets and constraints**: implement science-based net-zero targets for the ICT sector, enforced through incentives and compliance mechanisms. All this can be achieved by encouraging credible carbon pledges and ensuring that all companies within the sector are held to similar standards.

DIGITAL INDUSTRY 5.0

(e.g. Internet of Things and Cloud Computing) and digital business/companies

- **Regulations have to be informative and precise** to provide a predictable and stable legal framework that enables innovation to take place.
- Regulations should aim at **enabling European digital innovation** in order to be **competitive on the global digital market**, whilst also **providing safeguards and enforcing penalties** on companies which unlawfully distort competition or are in breach of the norms.
- Dedicated funding opportunities for **open-source technology and educational platforms** must be ensured.
- Alliances under the Important Projects of Common European Interest (IPCEI)⁴⁵ and Digital Innovation Hubs for the sharing of knowledge and best practices should be diversified to **include more small and medium-sized**

enterprises (SMEs) from peripheral regions of the EU, and their outreach and communication need to be improved.

- The EU should **establish a central pool of advisors** who can be requested by smaller companies to advise them on what can be improved (advocating open source, enabling knowledge sharing, sustainable practices, etc.).
- The European Institutions and public bodies should avoid using taxpayers' money to unilaterally adopt and implement communication tools, early-stage technologies, and prototype platforms that do not serve a general interest of European citizens. Instead, they should **facilitate a positive engagement with civil society, stakeholders and citizens** in order to identify the positive effects the adoption of a particular digital product or service can have on society as a whole

2.3

Digital Rights and Freedom

Defending and protecting the right of everyone to have an access to secure and sustainable technological infrastructures. Concepts include:



1. DIGITAL CITIZENSHIP:

The development of a framework of digital rights and principles that will help promote and uphold EU values in the digital space.



2. DIGITAL SERVICES:

The right to fair, transparent and accountable digital services' content moderation processes.



3. ONLINE PRIVACY:

The level of privacy protection an individual has while connected to the Internet.



4. E-INFORMATION:

The right to access information given by governments, companies, etc.



5. NET NEUTRALITY:

The right to Internet access which should be offered to everyone on a non-discriminatory basis, without favouring certain websites, applications or services.



6. DATA (PROTECTION AND RETENTION):

The right to data protection and knowledge about data retention.

7. COPYRIGHT:

Traditionally, the exclusive and assignable legal right, given to the originator for a fixed number of years, to print, publish, perform, film, or record literary, artistic, or musical material. In the digital age, copyright should be implemented in a way which benefits creators and society.

8. ONLINE SAFETY OF JOURNALISTS:

ensuring plurality of voices in digital media markets.

9. PROTECTING FUNDAMENTAL RIGHTS IN ONLINE ENVIRONMENTS.

MAIN CHALLENGES:

- ➔ ENSURE ACCESSIBILITY OF DIGITAL INFRASTRUCTURE AND TOOLS TO THE ENTIRE POPULATION
- ➔ ENSURE INCLUSIVENESS AND EQUALITY
- ➔ ENSURE CORRUPTION AND CENSORSHIP DO NOT OCCUR IN REGARD TO CONTROL OF DATA AND FREEDOMS ONLINE
- ➔ ENSURE ONLINE PRIVACY AND DATA PROTECTION
- ➔ ENSURE NET NEUTRALITY

RECOMMENDATIONS:

ONLINE PRIVACY AND DATA (PROTECTION AND RETENTION)

- EU institutions should **ensure enforcement of existing legal frameworks**, such as the General Data Protection Regulation (GDPR), the Digital Services Act (DSA)

and the EU Code of Conduct on Disinformation and update the ePrivacy Directive with a strong ePrivacy Regulation.

- Sound implementation and enforcement of the legislation in an inclusive, transparent manner that **enhances the protection of fundamental rights, civic discourse and electoral processes**.
- **Ensuring the privacy of disability and health-related sensitive data** is vital. Many websites can detect if a person is using assistive technology (e.g. screen reader) to access them. This means a person's disability can be revealed against their will, which can lead to algorithmic discrimination (e.g. targeted ads about vacancies, services, avoiding persons with disabilities) or discrimination and harassment by entities and individuals possessing that data.

NET NEUTRALITY AND DIGITAL SERVICES

- **Net neutrality** should be protected by law to guarantee the free and fair sharing of content online.
- EU institutions and Member States should **address the rising Internet centralisation** and focus on how to prevent a few giant global companies from running most of the services (end-user applications, application stores, device neutrality, infrastructure) and holding most of the data. It is important to restore competition through regulation (e.g. the European Digital Service Act and Digital Markets Act) and through open source, open standards and interoperability.
- The EU needs to **monitor any attempts to introduce practices such as zero-rating that undermine net neutrality**, and take regulatory action where needed.
- Moreover, the EU needs to encourage innovation at the EU level to **support the creation of EU platforms and service providers**, which are appealing to users, competitive, and conform to EU standards and values.
- To ensure online freedom, the EU should consider **eliminating geo-blocking** and **enabling multilingual/national broadcasting** with access to subtitles and different language audio tracks.

PROTECTING FUNDAMENTAL RIGHTS, SECURE AND SUSTAINABLE DIGITAL INFRASTRUCTURES, DIGITAL CITIZENSHIP, ONLINE SAFETY OF JOURNALISTS AND ENSURING PLURALITY OF VOICES IN DIGITAL MEDIA

- The **EU's digital policy should undergo an overarching reform** in order to strengthen its accountability and transparency in digital technology markets and protect fundamental freedoms and human rights. Strong regulation should be implemented by well-resourced and independent enforcement agencies, while encouraging and supporting authentic innovative EU alternative solutions.
- **Protecting encryption as a means of self-protection** is a fundamental aspect of private communicators' rights (especially for human rights defenders and marginalised groups) and must not be unduly restricted. This includes the right not to supply any authority with passwords or encryption keys and current attempts to undermine encryption in the Child Sex Abuse Regulation.
- **Build public digital infrastructure** (such as Internet connection) and **ensure its financial sustainability**, especially with regard to access to equipment for people facing material deprivation (e.g. low-income households, the homeless).
- **Ban mass surveillance and facial recognition technologies** as they fundamentally undermine an enabling environment for democratic societies, threatening political pluralism and civil and political rights.

COPYRIGHT

- The EU should **reform the Copyright Directive** to allow exemptions for persons with disabilities to access e-books, films and music.

2.4

Digital Safeguards

The safeguards EU decision-makers need to put in place to ensure the respect of values, ethics and norms in the digital space (e.g. EU policies, regulation, etc.). These include:



1. CYBERSECURITY:

The protection from hackers, fraud, viruses etc. and managing risks of hybrid attacks.



2. ARTIFICIAL INTELLIGENCE:

An AI that is ethical and that protects people, communities and society from the escalating economic, political and social issues posted by AI.



3. ALGORITHMS:

Transparency of algorithms.



4. ONLINE DISINFORMATION PROTECTION

against false, inaccurate, or misleading information used to intentionally cause public harm or make a profit.




5. AUDIO-VISUAL MEDIA SERVICES:


Regulation of online content and the role of online platforms in disseminating it as it has a direct impact on freedom of expression and access to information.



6. INTEGRITY OF ELECTIONS:

Protection of the integrity of elections and promotion of democratic participation.

-  **7. ONLINE HATE SPEECH:**
Prevention of practices that denigrate people, based on their race, ethnicity, gender, social status, etc.

-  **8. ILLEGAL CONTENT ONLINE:**
Measures to effectively tackle illegal content online.

MAIN CHALLENGES:

-  **ENSURE CYBERSECURITY**
-  **ENSURE THE ETHICAL USE OF AI**
-  **TRANSPARENCY OF ALGORITHMS**
-  **MONITORING OF ONLINE DISINFORMATION**
-  **ENSURE ACCESSIBILITY**
-  **MONITORING ONLINE HATE SPEECH**

RECOMMENDATIONS:

CYBERSECURITY

- There should be **publicly funded, easily accessible and free-of-charge public education about cybersecurity** available to all European citizens, to help protect them from harm.
- The EU needs to **step up investments into cyber security**, both for the purpose of elections and also beyond elections.

ARTIFICIAL INTELLIGENCE

- **AI** – automated decision-making must be **transparent and subject to human review** when operating in the public sphere with a potential impact on society and subjected to public scrutiny. Proactive regulatory actions and funding opportunities should promote public AI that will bring tangible benefits to citizens – for example, promoting the development of AI-based assistive technologies for persons with disabilities or ensuring diversity is part of the AI design. Communities affected by the impact of AI should be involved in its development as part of their human rights due diligence.
- **The EU's AI Act must be adopted** to ensure at least the following principles:
 - 1) include sufficient safeguards to protect citizens from any negative impact of AI technologies on their fundamental rights, particularly ensuring privacy, accessibility, and non-discrimination; 2) uphold an effective right to redress for those affected by an AI application and raising awareness and accessibility to redress mechanisms; 3) make human rights impact assessment mandatory for the design, development and deployment of AI.
- The EU needs to **develop a framework that determines the extent, type, form and moment of human intervention in AI automated decision-making**. Within this framework, one of the determining criteria should be the impact of AI on rights, duties and liberties.
- Furthermore, the EU should **regulate AI systems, including in those areas that fall under the remit of the Common Foreign and Security Policy** (e.g. for military purposes), and provide a harmonised horizontal legal framework with common rules and safeguards to ensure that all systems are accurate, robust, secure, and function according to their strict specifications.
- The **European Data Protection Board (EDPB) should keep working in close cooperation with national authorities** toward common, transparent and inclusive standards and policy on privacy rules and AI.
- The EU should **support research and efforts to make AI more explainable to citizens** and align the strategies pursued by AI systems with good behaviour.

- The EU should **raise awareness about the functioning and capabilities of AI systems** (and the limits thereof), and dissuade too strong claims about the capabilities of an AI product.
- In addition to the already proposed regulatory measures, the EU should aim at the **establishment of complementary initiatives**, such as certification and codes of conduct in any AI-powered systems, with benefits for the companies acting, on a voluntary basis, in compliance with them.
- Further investment and measures to **mitigate the effects of automation in affected sectors** e.g., in retraining of people that see their field of work displaced by rapid technological advancement.

ONLINE DISINFORMATION, INTEGRITY OF ELECTIONS, TERRORIST CONTENT, ONLINE HATE SPEECH, ILLEGAL CONTENT ONLINE

- **Online content moderation** should ultimately always require a form of human review and intervention. The appropriate type, form and moment of this human intervention should be considered on a case-by-case basis, taking into account the impact of AI automated decision-making on individual rights, duties and liberties. To counter disinformation, illegal content and hate speech online, EU institutions and Member States must combine their financial instruments in support of civil society and the media with legislative instruments holding online platforms to account while safeguarding fundamental freedoms. Social media platforms must be encouraged to take measures to prevent smear campaigns spreading disinformation, online harassment and abuse against civil society, journalists, women, non-binary people, racialised people, LGBTQIA+ people, persons with disabilities, children and all others at risk of cyberbullying. Yet such measures must always serve to defend people's freedom of expression and association, as well as media pluralism and editorial independence.
- EU institutions and Member States should **provide support – technical, policy and financial – for those civil society organisations** countering online hate speech, protecting survivors and conducting independent media and fact-checking; and those providing digital literacy education for citizens, including education on cybersecurity and AI.

- Moreover, EU institutions and Member States need to **defend fundamental freedoms and deter illegal hate speech** by including an online content moderation regime that requires a form of human review and accessible and clear criteria – agreed amongst diverse stakeholders – for the removal of restrictions on content (in the Digital Services Act).

EU'S DATA ACT

- **The EU's Data Act should be further improved**, since it currently sets a controversial precedent by allowing public authorities to access private data during emergencies. Moreover, as public officials often move from the public to private sector, there is a risk of potential conflict of interest, which needs to be adequately addressed by the legislator.

ALGORITHMS

- **Transparency of algorithms** – all public and private users of automated decision-making should also be required to provide detailed information on when they use automated processes (whether algorithmic or otherwise) to moderate third-party content and how such mechanisms operate. This information should be made available in public registers. In addition, redress mechanisms for those affected by algorithm-based automated decision-making should be a requirement while awareness raising of the redress mechanisms is a must.
- Consider **transparency requirements** regarding dynamic pricing, targeted advertisements and campaigning.

DIGITAL FOR DEVELOPMENT

- **The Global Gateway should be progressively scaled up** in order to create long-lasting partnerships with third countries based on democracy, EU values and Team Europe approach, particularly in areas related to digitalisation and infrastructures.

- **Digital Development (D4D) Hubs should be continuously supported** by both the European Commission and the member states, in order to facilitate a global dialogue with stakeholders across the globe based on a human-centric approach to digital transformation.

2.5

Digital Education

Resetting education and training for the digital age - the digital divide must be addressed not only through the accessibility and availability of infrastructures and technologies but also through the possibility of digital education for all. Concepts around digital education include:



1. DIGITAL COMPETENCIES:

The set of basic digital skills, covering information and data literacy, online communication and collaboration, digital content creation, safety and problem solving.



2. DIGITAL SKILLS:

Job related skills or Digital skills for ICT professionals.



3. DIGITAL LEARNING:

The innovative use of digital tools and technologies during teaching and learning.



4. MEDIA LITERACY:

The skills that allow people to access, critically evaluate and create or shape the media.



5. AWARENESS RAISING:

Informing and communication to citizens about digital practices.

MAIN CHALLENGES:

- ➔ ENSURE ACCESSIBILITY
- ➔ ENSURE DIGITAL LITERACY FOR ALL CITIZENS
- ➔ DATA PROTECTION

RECOMMENDATIONS:

DIGITAL SKILLS AND COMPETENCIES

- EU institutions and Member States should **support the development of a learner-centred approach to digitalisation in education**, including EU-level policies to support education systems so that they have bargaining power in relation to Ed Tech, as well as legally binding rules on using AI and data privacy in education, including through a comprehensive implementation of the Digital Education Package.
- **Resources for fostering digital skills should be targeted at those who are more strongly affected by the digital transition** (such as students and persons with disabilities, NEETs, refugees, low-skilled adults, ex-prisoners, single women, low-income households and people facing social exclusion) and should also address existing barriers (e.g. lack of accessibility). EU institutions and Member States must ensure that the digital transition does not exclude anyone and **strive to further reduce the biases that go into the design of digital technologies** by expanding perspectives.
- Although digital competencies and skills can be a valuable route into employment (including for vulnerable groups), their scope should not be limited to technical skills only, but should also **include soft skills, netiquette, empathy, sustainability, ethics, media literacy, dealing with false or biased information, targeted advertisement, pricing and campaigning, spotting of deceptive design patterns and skills related to content accessibility**.

MEDIA LITERACY AND DIGITAL LEARNING

- **Media literacy should be for all parts of society** (e.g. it should foster social inclusion and the public communication and discussion thereof).
- **Strengthen civic education and confidence building** in the areas of active citizenship, democracy, European and national competences, populism, online and offline disinformation, news, media and digital literacy, EU fundamental rights and values, and respect for minorities.
- **Privacy and data-protection knowledge** should also be developed through dedicated programmes – **tailor-made to specific target groups** e.g. young people and elderly people.
- **Digital knowledge, skills and competency building should be incorporated into formal education** curricula as well as part of the large-scale objective of bringing education into the 21st century (including lifelong learning and informal education).
- Although digital technologies may be instrumental in improving education, **education through digital means should not be of a lower quality compared to non-digital traditional education** and ensure that nobody is left behind when it is necessary to participate in online learning. .
- **Training and EU programmes on a wide range of digital skills** (e.g. technical, ethics and soft skills) **should be developed** ensuring that they are tailored to the needs of those citizens in a vulnerable position, including persons with disabilities, elderly people, NEETs, refugees, low-skilled adults, single women, low-income households and people facing social exclusion, and ensure adequate and continuous funding for such actions.
- **Teachers and public administrations should also be trained** in the essentials of digital technologies, digital skills, software and algorithms to foster a greater understanding, better discussion and handling thereof and the transmission of knowledge. It is necessary to **enable the proper circumstances for such training** in order not to overburden them and provide incentives to attend such training.

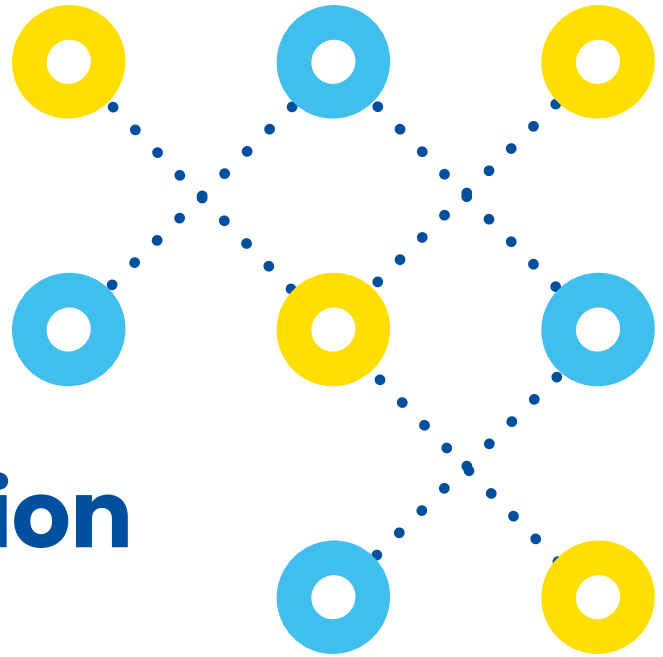
- **Non-formal education trainers should be consulted** when developing digital education plans at both the European and national level.
- We need **more EU-funded programmes for civil society organisations** to support the development of digital education strategies (especially with regard to digital skills and competencies beyond formal education) based on a lifelong learning approach.

AWARENESS RAISING

- Public programmes concerning the development of digital skills and competencies should **rely on civil society organisations and local initiatives** as mediators and entry points.
- The **cross-sectoral collaboration** between scientists, civil society, governments, companies and media on issues concerning digitalisation needs to be **improved and supported financially**.

3.

Digital Inclusion Guidelines



Based on the Civil Society Recommendations on Digital Transformation, in 2022 and 2023, ECAS held co-creation events to collect ideas for more digital inclusion in Europe from a wide array of stakeholders in 10 countries: Ireland, Portugal, Latvia, Luxembourg, Belgium, Germany, Greece, Italy, Croatia and Bulgaria. Participants were a combination of citizens, experts, policymakers and NGO representatives, who had the chance to dive deeper into the topics previously mentioned of Digital Democracy, Digital Economy, Digital Safeguards, Digital Rights and Digital Education. These concepts were presented by ECAS to participants to explain the EU level and commented on by national experts to give an overview of and context at the local level.

In the first part of these events, participants had the opportunity to familiarise themselves with the challenges towards inclusion and the main recommendations from CSOs in each area and were informed about relevant EU digital policies and current debates.

In the second part, we asked participants to answer a set of questions that led to discussions around the civil society recommendations, and they responded with

their input, mainly on digital inclusiveness, by sharing their daily experiences with digital technologies and the issues they face as Internet users. Participants provided their own recommendations for the EU digitisation process in order for it to include all EU citizens, with a special focus on those who are digitally excluded, marginalised and underrepresented.

The questions administered to participants at (and/or prior to) all events led to comparative results amongst the countries involved. The same questions were repeated across all 10 Member States, allowing for comparison and analysis of the contributions of the participants. To engage more effectively with participants of Member States who may struggle with the English language, in a few cases, the questionnaire was translated into the local language and/or the event was implemented in the local language (for instance, this was the case of the events in Croatia, Italy and Bulgaria in 2023). At all events, however, participants were also invited to contribute to open-ended questions in their own language, if needed or preferred, in order to facilitate engagement and ensure accessibility. ECAS and the partner organisations focused on engaging different groups in the co-creation exercise. Inclusive recruitment of participants enabled this EU-wide effort to be representative of a diverse range of EU citizens. A few examples were the events in Luxembourg (the older population), Italy (the younger population), Germany (migrants), Greece (local CSO representatives and volunteers), and Ireland (women), where a considerable percentage of the participants were from a vulnerable and socially and/or digitally excluded groups. Furthermore, ECAS and local organisers invited women (experts, CSO representatives, and policymakers) as guest speakers to further promote their visibility and empowerment in the field of Information and Communication Technology.

The common experiences amongst Member States around the challenges of digital transformation showed the need for stronger policy intervention at the national and EU level to ensure that the digital transition is an inclusive process that leaves no one behind. In the following subchapter, we present the guidelines for more digital inclusiveness in Europe based on participants' recommendations summarised into two broad areas: **Infrastructure Requirements and Supporting Ecosystem.**

3.1

Infrastructure requirements: Resources, Security and Design

The infrastructure requirements concern the resources and processes that ensure the accessible design of online services and the necessary measures to provide security.

Regarding the identified resources that would ensure the accessible design of online services, the most prevalent recommendations from participants are the following:

- ✓ **Free, accessible, high-speed Internet available to all;**
Good-quality Internet connectivity should be a public good.
Free Internet connectivity and devices should be available for use in public spaces.
- ✓ **Regular audits evaluating the accessibility of content of websites, online services and new features;**
Information should be easy to find and there should be Intralinks allowing users to access what they need from different parts of the websites/apps. Navigation should be made as intuitive as possible for users of different degrees of knowledge of the subject they are searching.
- ✓ **Simple and concise information available on websites of public administrations, banks, healthcare system, etc.;**
Information and tools (apps, platforms, authentication systems, etc.) should be in a simplified format and language for easy navigation (avoid bureaucratic and/or technical language, provide glossaries), and include translations into languages spoken by national linguistic minorities and other non-native speakers.



Regular update of displayed information, optimisation of processes and fast bug-fixing;

Websites and apps of public administrations should be regularly tested against server failure and general navigation issues.

Participants also shared their frustration towards e-services of public administrations not being fully online, which nullifies the benefits of such services as a whole. In some cases, for instance, it is still required of citizens to submit documents previously downloaded online in person in administration offices, or vice versa documents may have to be requested in person but can be signed and sent back via email.



Dedicated staff to support the users of a website;



Dedicated staff (chat boxes / FAQs sections / helpdesks / physical offices) for digital governmental services (and other services, such as banks and the healthcare system) to support citizens.

No automatically generated responses, availability of human agents.

Support formats tailored to the needs of specific populations, especially for vulnerable groups.

Moving to the requirements surrounding the design of the website, participants proposed:



Developing collaborative and bottom-up processes that will ensure user-centric design of online platforms;

With high standards of quality - equal standards to the services provided by private company online services.



The design process should include various user personas;

Ranging from digital native users to individuals with certain vulnerabilities such as people with visual impairments, audio impairments, the older population, and children. Each target audience should be included in the

design process, in particular underrepresented and digitally marginalised groups.



Simplified structure of information;



Governmental services must have mobile app versions;

Some argued the opposite – that the number of apps a citizen needs is getting out of hand. Therefore service providers should seek a balance in multi-use apps with easy-to-find features.



Compatible with screen readers and following accessibility guidelines;

Option for magnifying font size – user mode differentiation based on whether it is an older person, a person with disabilities, etc. In general, ensure accessibility provisions for the older population, people with disabilities, destitute people and other vulnerable groups (e.g. residents of rural areas, people with lower education levels).



Single sign-in with interconnected governmental services;

One-stop-shop for most public administration online services to simplify access to information and communication amongst different areas. In general, avoid fragmentation of public online services.



Privacy should be a primary concern;



Protect against threats deriving from Artificial Intelligence.

Participants shared concerns regarding Artificial Intelligence and how it can cause further discrimination and threaten EU citizens' rights. Participants called for stricter rules and regulations regarding the transparency of algorithms. Human oversight was a recurring request across the countries polled. Participants also stressed the need to include marginalised and underrepresented groups in the programming and monitoring process.

Finally, to ensure security, participants recommend:

Prioritise cybersecurity to reinforce the trust of citizens in digital tools;

Participants suggested that strengthening security measures and sanctions for data misuse would help them feel protected from threats when navigating online. They also recommended acting preventively, and not only after “the damage is done” – participants mentioned actual cases of security breaches of governmental services in their country.

Security should not be at the expense of privacy and democratic principles;

Harnessing the potential of digital technologies for public security should not be to the detriment of citizens’ fundamental rights. Also, technologies such as facial recognition bear the risk of biases and discrimination, thus further increasing marginalisation and inequalities.

Simple and concise written information on how the data is stored, to what use(s) and if it will be provided to third parties.

To build citizens’ trust in digital technologies, online data sharing must comply with rules and regulations regarding many aspects, from clarity of information provided to the users to set limitations on how, why, when and to whom the data would be shared. The need for transparency on online platforms, websites and services was a recurring issue in the participants’ recommendations. Participants declared that they are mostly unaware of what happens to their data online and this is a cause of concern. Accepting terms and conditions is often met with a feeling of resignation before complex and long texts, or avoided completely out of uncertainty or fear. At the same time, some participants warned that people may underestimate the risks due to a lack of awareness or understanding, which may lead them to potential threats to their online security and that of others.

3.2

Supporting ecosystem: Assistive services, Education initiatives, Communication campaigns

The supporting ecosystem will ensure that socially excluded groups have the required assistance to navigate through the digital world and develop their digital competencies as empowered citizens. It can be summarised in three broad areas of societal action: Assistive services, Education initiatives, and Communication campaigns.

According to participants, there needs to be more supply in all geographic regions for assistive services that will help individuals from diverse backgrounds use digital tools, get familiar with them and, at a later stage, use the transformational value of such tools in all aspects of their daily lives.



Physical spaces;

Initiatives aiming to develop a supportive ecosystem for the digitally excluded should provide a physical space. A safe space where people can find digital literacy and digital health training, receive in-person digital assistance and feel they have a secure environment to develop their digital activities (civic activities, consumer activities, learning and development activities).



A targeted supporting ecosystem should be tailored to destitute people's needs and other vulnerable groups;

The existing centres for destitute people should not only provide technological tools and Wi-Fi access but also possibilities to obtain a digital education. Participants suggested that nursing and retirement homes and other facilities for the older population should also offer opportunities

to access technological devices and the Internet, and acquire a digital education.



Funding to CSOs that can support the digital inclusion of vulnerable groups.

CSOs are the best-suited actors to initiate and mediate digital inclusion activities and campaigns, in virtue of their direct experience engaging with vulnerable groups, listening to their needs and tailoring programmes that respond to them with a hands-on and bottom-up approach. Also, CSOs should be the first interlocutors for governments planning to design policies and programmes that do not further increase the digital divide or create new inequalities through digital technologies.

Participants provided suggestions on the development of education initiatives which currently are, according to them, limited in quantity, insufficiently accessible and overall not well known to the public.



A more holistic approach to digital literacy, which should be accompanied by other fields of literacy (financial literacy, civic literacy, cybersecurity literacy, consumer literacy);

This is the most efficient way to integrate various digital tools into citizens' everyday lives. Increased literacy should also aim at increasing the users' confidence in identifying security threats, online hate and disinformation. Literacy programmes should consider the specific needs of digitally excluded and vulnerable groups, such as the older population, children and young people, the socially and economically disadvantaged, people with disabilities, people with lower education levels. Also, participants suggested that literacy programmes should be designed for employees of public institutions and administrations, teachers of all levels, and entrepreneurs (SMEs).



Online 'fire alarm' drills, such as sending real phishing tests to citizen emails;

This is a training practice often used in big corporations to train their employees in potential tricks used by malicious individuals. Phishing emails

aim to retrieve specific information and get receivers to download malware. Companies imitate such emails and keep score of failure to ignore such attacks – leading to a gamified approach. This, apart from training the receivers to recognise potential threats, also keeps their alert level high against potential malicious emails.



The focus of financial digital literacy should be on fraud avoidance;

Identifying phishing, false ads, malicious intent in general, and developing a basic security skill set is not only part of media and cybersecurity literacy, but a fundamental need for sufficiently financially literate citizens.



Introduce media literacy in formal education, starting from school, and discuss about it in the media;

Introduce digital literacy in compulsory school curricula, starting from an early age. These initiatives must not only be sporadic and driven by the goodwill of some teachers, but rather the result of structured planning at a national level, which first covers the training of teachers, and which should then reach the students.



Recognising the importance of lifelong learning;

Training programmes for adults should take place in local hubs. According to the comparative analysis, NGOs and public institutions should lead such initiatives, focusing on providing free-of-charge, group-specific and accessible training opportunities. More financial support should thus be allocated to such entities to enable them to develop and deploy high-quality training to all citizens who may need it. At the same time, an overwhelming majority of participants stated that, when needing help to navigate the digital world, they turn to a friend or a family member for support. Trust in and awareness of State- and/or EU-funded resources should thus be increased among EU citizens. Participants suggested incentives could be used to encourage citizens to participate in training courses (e.g. include such training in working hours for employees, grant tax exemptions, or other forms of reward).

✓ **All Digital Education opportunities should comply with Web Content Accessibility Guidelines (WCAG) 2.2.**

Training providers should partner with organisations already working in this field.

Another recurring theme throughout all focus areas in all participating Member States was the one proposing new communication approaches.

✓ **Targeted communication campaigns to promote e-participation tools;**

To improve civic digital literacy, providers and governments should develop targeted communication campaigns and educational initiatives for governmental and e-participation tools, and in general on the importance of citizens' empowerment in the digitalisation process. To maximise their impact, such campaigns and initiatives should target the different vulnerable groups, also in their language (in the case of linguistic minorities), and communication channels of different kinds (traditional media, online platforms, the education system, external collaborations with CSOs and other social actors as mediators and multipliers). Public awareness-raising programmes should also focus on encouraging and motivating those citizens who may not trust the technologies or governments/public administrations (in the case of e-government). More efforts are needed to ensure that citizens can trust that their data is secure and, for e-participation initiatives, that their voices are heard. In this sense, some participants also asked for more crowdsourcing and other e-participation initiatives.

✓ **Targeted communication campaigns on the Commission's actions that ensure citizens' data and privacy are protected online;**

This recommendation derives more from the identified lack of awareness of citizens of digital education opportunities rather than from their explicit recommendations. However, participants repeatedly stressed how important it is to be aware of the risks and threats one can incur when using digital technologies, in terms of data protection, security, disinformation, false

advertisement and frauds, inappropriate or violent content, and online hate, amongst others. This highlights the need to develop campaigns to raise awareness of the debates and advancements in this area at the EU level.

✓ **Create a digital ambassadors programme which would drive a focused campaign to reach out to a variety of vulnerable target groups nationwide;**

✓ **Gather live and real experiences from the vulnerable groups themselves in order to create well-informed solutions.**

The direct involvement of representatives of vulnerable groups in policymaking processes and in the planning of programmes and campaigns is the first step to effective digital inclusion. This is a cross-cutting recommendation received by the participants of all events. In order to design future initiatives that leave no one behind, those who are now digitally excluded must sit at the table and have their voices heard.

The EU's Digital Transformation 2030

Civil Society
Recommendations
& Digital Inclusion
Guidelines

ECAS Brussels, April 2024

European Citizen Action Service

BeCentral, Cantersteen 12

B-1000 Brussels, Belgium

✉ info@ecas.org

✂ [@ecas_europe](https://twitter.com/ecas_europe)

f [ecas.europe](https://www.ecas.europe)

in ECAS – European Citizen Action Service

