# Digital Transformation Cluster
## Final Recommendations

## Background

The Civil Society Convention's **Digital Transformation Cluster** has worked on developing proposals that will feed into the EU's priority of "A Europe fit for the digital age". The ambition of this priority is 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. In order to ensure a **digital transformation in Europe that leaves no one behind**, the Cluster focused its work on five main topics: *digital democracy, digital education, digital safeguards, digital rights and freedoms* and *digital economy* (Annex - Glossary).

Digitalisation is becoming ever more ubiquitous and indeed 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 have often the possibility to engage in democratic life through e-participation channels. In the last decade, the EU focused its e-government and e-transparency efforts on technological solutions for public administrations, businesses and people (e.g. electronic identity). On e-participation, there are a few existing channels that play an important role in citizen engagement, such as the European Citizens' Initiative. However, these channels are not sufficient for a meaningful involvement of EU citizens and there is a need for **e-participation tools to be more inclusive, used in a structured way, accessible for everyone, and especially more impactful**.

On the other hand, citizens are also now part of a society more and more focused on **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 among the most profitable and have impacted all of Europe, 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.

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. Digital policies have been one of the cornerstones of EU legislation since 2019, with the European Commission proposing several new regulatory frameworks – Artificial Intelligence, ePrivacy Directive, Digital Services Act (DSA), the Digital Markets Act (DMA) and the Data Governance Act (DGA).  In 2021, the European Commission presented a vision and avenues for Europe's digital transformation by 2030 in its Digital Compass for the EU's digital decade that evolves around four cardinal points: government, skills, infrastructures, and businesses.  Although the EU has declared to set ambitious targets, frameworks and projects to ensure Europe's digital development, Civil Society Organisations (CSOs) have raised concerns about the impact of the 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. In order for Europe to be a front runner in the digital domain, the EU 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 – people with disabilities, seniors, migrants, homeless people, people at risk of poverty and social exclusions, women and many more. For this reason, the EU should make the access to **affordable, highspeed Internet a fundamental right** for its citizens. If access to the Internet is guaranteed and accessible **digital education is made a priority and is evenly implemented across all Member States in order to equip people with the right skills and competencies**, this will result in increased citizens' involvement, especially in the digital democracy and the digital economy of Europe.

Digitalisation will only advance European societies if we **can safeguard and strengthen our democracies in the process**. To this end, there are several digital policies still needed at the EU level to ensure digital technologies are developed and used in respect of human rights and democratic principles. Various EU legislative processes are currently attempting at putting in place safeguards to human rights while stimulating innovation and market integration (including 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 center of these legislative processes, alongside innovation and competition concerns**. For example, AI respecting fundamental rights must be allowed to develop in the EU, or else it will be developed in other parts of the world with far fewer safeguards.

In conclusion, European digital policies are a mix 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 people versus Big Tech. However, the EU's effort is simply not enough. CSOs are raising concerns regarding privacy issues, the surveillance of people, such as asylum seekers, racism in AI 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.**

## Methodology

The Digital Transformation Cluster was led by Elisa Lironi, Senior Manager at the **European Citizen Action Service (ECAS)**, who developed and elaborated the final recommendations together with the Working Group members of the Cluster:

- Alice Stollmeyer (Defend Democracy);
- Andrea Castagna (European Digital Development Alliance);
- Andrei Frank (SOLIDAR);
- Aoife Curtis (European Partnership for Democracy);
- Berna Keskindemir (European Centre for Not-for-Profit Law);
- Corinne Szteinsznaider, (Michael Culture);
- Diego Naranjo (EDRI);
- Dominik Kirchodofer (European Future Forum);
- Elizabeth Gosme (COFACE);
- Eva Lichtenberger (Union of European Federalists);
- Ildmila Nemocovà (European Anti-Poverty Network),
- Lisy Piter (ALDA);
- Marie-Luise Abshagen (SDG Watch Europe);
- Mher Hakobyan (European Disability Forum);
- Robert Scholz (European Future Forum);
- Ruth-Marie Henckes (European Partnership for Democracy);
- Sergio Pérez Barranco (FEANTSA);
- Simon Delakorda (Institute for E-Participation, Network NVO-VID Slovenia)
- Stefan Cibian (Arcadia Network)
- Vanja Škorić (European Centre for Not-for-Profit Law).

The elaboration of the Convention's Digital Transformation proposals went through a Crowdsourcing process that included 4 different phases:

- **Phase 1 Ideas Collection** (Jul-Nov 2021) – The Crowdsourcing Platform allowed CSOs to propose ideas (one or two sentences max) about Europe's digital transformation. These ideas were statements under the specific topics and subtopics (ANNEX), mainly
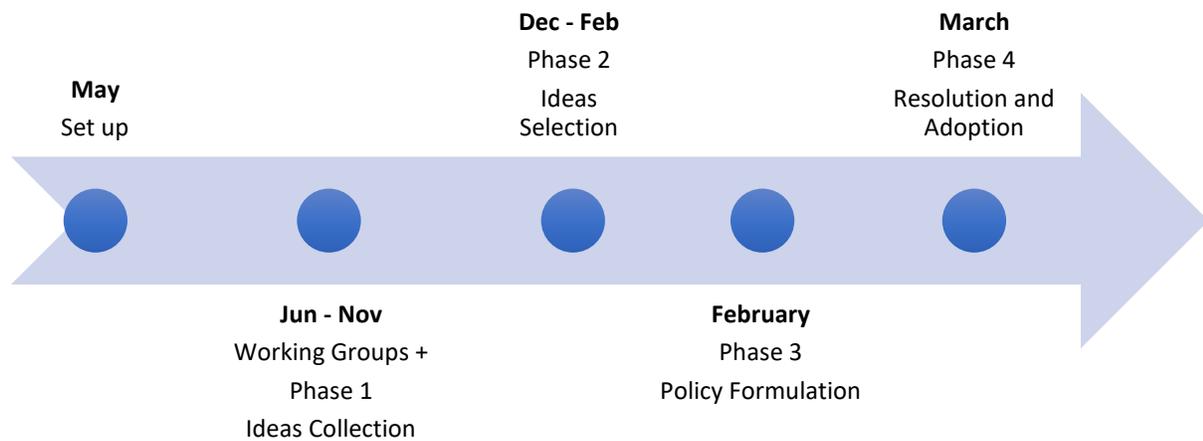
the priorities they think the EU should focus on in the next few years. The Ideas Collection phase was implemented in two steps: first, the Working Group members of the Cluster had the possibility to submit their proposals on the platform; second, the platform was open to CSOs across Europe to collect their ideas on the topics.

- **Phase 2 Ideas Selection** (Dec-Feb 2021) – CSOs were called to use the Crowdsourcing Platform to go through all the ideas and to rate/select the best ideas according to them under the different topics. Each topic had a limited amount of votes in proportion to the contributions submitted in the first phase.

- **Phase 3 Policy Formulation** (Feb 2022) – The top ideas were     chosen as priorities and each topic had one CSO leader from the Working Group help formulate a common position.

- **Phase 4 Resolution and Adoption** (Mar 2022) – ECAS in collaboration with the CSOs leaders of the topics developed a resolution with the top ideas and the Working Groups members adopted the final resolution together.

20 Civil Society Organisations and 7 individuals participated on the Crowdsourcing platform, generating a total of **216 ideas and recommendations** that were distributed between the 5 subtopics of digital transformation (Digital Democracy, Digital Economy, Digital Education, Digital Safeguards and Defending Rights & Freedoms Online). The Working Group members are all network organisations that represent a total of **approximately 1200 CSOs across Europe**.

A flagship initiative of

## TIMEFRAME

**May**
Set up

**Dec - Feb**
Phase 2
Ideas
Selection

**March**
Phase 4
Resolution and
Adoption

**Jun - Nov**
Working Groups +
Phase 1
Ideas Collection

**February**
Phase 3
Policy Formulation

The following sections include the final recommendations and proposed actions for the EU.

# Digital Democracy Recommendations

*Subtopics: E-Government, E-Transparency, E-Participation, E-voting/E-elections.*

- E-government solutions should be developed in **consultation with the end users and civil society organisations** to ensure solutions are **accessible and inclusive** of all people, efficient, trustworthy, safe, subject to privacy and controlled by humans.
- Alternatives to e-government services must be provided to ensure that those that do not have the possibility to use digital tools, and people with disabilities or with a low digital literacy can still be adequately engaged and served adequately.
- E-government public data and documents at 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 used language and its finding place.
- In order 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 easy to read format. The platforms, tools and technologies to access this information should be accessible as well. Citizens must always have the option of non-digital access to information.
- The EU institutions and governments should actively promote and clearly communicate e-participation in decision-making and provide citizens with a realistic opportunity to influence policy and legislation.
- European citizens capacities to engage in **e-participation** should be strengthened, as well as the impact their contributions make in policy-making. They should always receive feedback to what extent their inputs to decision-making are taken into account and why (or why not).
- The EU Member States and the European Parliament should proactively explore opportunities as well address legal, technical and societal challenges **of e-voting/e-elections** by promoting internet voting pilots and testbeds.

## Call to Action:

1. **Make** access to **free, equal and affordable Internet a fundamental right** of every EU citizen. Given the importance nowadays of having access to internet for a high number of vital tasks, access to internet should be guaranteed for everyone. In this respect, specific EU- and national-funded programmes could be allocated for vulnerable groups and people at risk of poverty or social exclusion to ensure they can afford internet.

2. **Provide public services that are fully accessible** for hard-to-reach segments of the population, through: a) **funding and collaborating with CSOs** that 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 its failures and successes.

3. Ensure that publicly financed software developed for public sector e-government solutions is made available under **a Free and Open Source Software license**.

4. Expand e-participation mechanisms and channels by **testing and combining new methods of citizen engagement** at the EU level e.g. crowdsourcing legislation and participatory budgeting.

5. **Pilot e-voting** at the next European Elections, provided it is technically secure, efficient and can guarantee transparency in the process.

# Digital Education Recommendations

*Subtopics: Digital Competencies, Digital Skills, Digital Learning, Media Literacy, Awareness Raising.*

- **Resources for fostering digital skills** should be targeted to those who are more strongly affected by the digital transition (such as students and people with disabilities, NEETs, refugees, low-skilled adults, ex-prisoners, single women, low-income households and people facing social exclusion) and also address existing barriers (e.g. lack of accessibility). The EU must ensure that 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 and skills related to content accessibility.**
- **Media literacy should be for all parts of society** (e.g. it should foster social inclusion) and the public communication and discussion thereof.
- **Privacy and data protection knowledge** should also be developed through dedicated programmes - with a specific focus on **adults and elderly people**.
- Digital knowledge, skills and competencies' 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, they should not become an end in themselves, nor should they replace non-digital ways of accessing education.
- Public programmes regarding 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 also supported financially.

## Call to Action:

1. Develop **training and EU programmes on a wide range of digital skills** (e.g. technical, ethics and soft skills) ensuring that they are tailored to the needs of citizens in a vulnerable position, including people 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.

2. Enable more **EU-funded programmes for CSOs** to support the development of digital education strategies (especially with regard to digital skills and competencies beyond formal education).

3. **Consult informal education trainers** when developing digital education plans both at European and national levels.

4. **Train teachers and public administrations** in the essentials of digital technologies, software and algorithms to foster a greater understanding, better discussion and handling thereof and the transmission of knowledge.

# Digital Safeguards Recommendations

*Subtopics: Cybersecurity, Artificial Intelligence, Algorithms, Online Disinformation, Audiovisual Media Services, Integrity of Elections, Terrorist Content, Online Hate Speech, Illegal Content Online.*

- 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.
- **Artificial Intelligence (AI)** - Automated decision-making needs to be transparent and subject to **human review** when operating in the public sphere with a potential impact on society, 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 A.I. design. Communities affected by the impact of AI should be involved in AI development as part of their human rights due diligence.
- **The EU AI Act** must be adopted to ensure the following points: 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.
- **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 the AI automated decision making on individual rights, duties and liberties. In order to counter disinformation, illegal content and hate speech online, the EU must combine its financial instruments in support of civil society and 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 persons, racialised persons, LGBTI persons, people with disabilities, children and all other persons 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.
- **The EU Audiovisual Media Services Directive** should require providers of audiovisual media services to ensure accessibility of audiovisual content for persons with disabilities.
- **The EU's Data Act** should be further improved - as it currently sets a controversial precedent by allowing public authorities access to 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.

- **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 and awareness-raising of the redress mechanisms is a must.

## Call to Action:

1. **Develop a framework that determines the extent, type, form and moment of human intervention in AI automated decision making.** In this framework, one of the determining criteria should be the AI's impact on rights, duties and liberties.
2. **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 specification.
3. **Provide support – technical, policy, financial - for CSOs** countering online hate speech, protecting survivors and conducting independent media and fact-checking; and providing digital literacy education, including education on cybersecurity and AI to citizens.
4. **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 removal or restrictions on content (in the Digital Services Act).
5. Include **more specific safeguards in the Digital Services Act[1] (DSA):** preventive measures, content moderation clauses, and sanctions to ensure that vulnerable and minority groups do not face discrimination online, on the basis of race/ethnic origin, sexual orientation, socio-economic status or disabilities.
6. Ensure that Member States **transpose and implement efficiently the Audiovisual Media Services Directive[2]** with legal quantitative and qualitative obligations for access services.

---

[1] More information: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
[2] More information: https://digital-strategy.ec.europa.eu/en/policies/audiovisual-and-media-services

# Defending Rights and Freedom Online Recommendations

*Subtopics: Secure and sustainable digital infrastructures, Digital citizenship, Digital Services, Online Privacy, Net Neutrality, Data (Protection and Retention), Copyright, Online safety of journalists and ensuring plurality of voices in digital media, Protecting fundamental rights.*

- The EU should ensure enforcement of the **General Data Protection Regulation** and update the ePrivacy Directive with a strong ePrivacy Regulation.
- **Ensuring privacy of disability and health-related sensitive data** is vital. Many websites can detect if a person is using an assistive technology (e.g. screen reader) to access them. This means a person's disability can be revealed without 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**[3] should be protected by law to guarantee free and fair sharing of content online.
- The EU should address the increased **internet centralisation** and focus on how to prevent a few giant global companies from running most of the services (end-user applications, app-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. Moreover, the EU needs to encourage innovation at EU level in order to support the creation of EU platforms and service providers, which are appealing to users, competitive and conform to the EU standards and values.
- In order to allow online freedom, the EU should consider eliminating **geo-blocking**, and enabling multilingual/national broadcasting with access to subtitles and different language audio-tracks.
- Protecting **encryption** as a mean of self-protection is a fundamental aspect of private communications' 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.
- 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.

---

[3] Net neutrality: the idea, principle, or requirement that Internet service providers should or must treat all Internet data as the same regardless of its kind, source, or destination (Merriem Webster)

## Call to Action:

1. **A strong ePrivacy Regulation[4]** should be adopted swiftly by the Member States, whilst also better enforcing GDPR nationally.
2. **Protect highly sensitive information** such as migration status, sexual orientation, race or any information on vulnerable economic conditions by: a) restricting access to this information as much as possible; b) limiting the requirement of this information for very exceptional cases; c) ensuring public decisions are not based in big data and biased algorithms.
3. Monitor any attempts to introduce practices such as zero-rating[5] that **undermine net neutrality**, and take regulatory action where needed.
4. Adopt an **ambitious Digital Service Act (DSA) and Digital Markets Act[6] (DMA**), which should include a ban on surveillance advertising[7].
5. **Ensure that encryption is protected** in the upcoming chat control legislation and in any other attempts to undermine it.
6. **Build public digital infrastructure** (like public charging stations & WiFi) and **ensure its financial sustainability**, especially with regard to access to equipment for people facing material deprivation (e.g. low-income households, the homeless).
7. **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.
8. **Reform the Copyright Directive** to allow exemptions for people with disabilities to access e-books, films and music.

---

[4] More information on the EU's ePrivacy Regulation: https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation
[5] 'Zero-rating' is when an internet service provider (ISP) applies a price of zero to the data traffic associated with a particular application or class of applications (and the data does not count towards any data cap in place on the internet access service). More info: https://berec.europa.eu/eng/netneutrality/zero_rating/
[6] More information: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en
[7] Surveillance advertising is the practice of extensively tracking and profiling individuals and groups, and then microtargeting ads at them based on their behavioral history, relationships, and identity

**A flagship initiative of**

# Digital Economy Recommendations

*Subtopics: Digital Industry 4.0 (e.g. Internet of Things, Cloud Computing, etc.), Digital Finance, Data Economy, Supporting Green Digital Solutions, Social welfare in the Digital Age, Digital Business/Companies.*

- 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.
- 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 reception of welfare benefits) have to be put in place for the European Single Market for data.
- The EU should ensure a **fair taxation of the digital economy across all Member States.**
- **Working conditions for online platform workers** have to be better regulated to address new forms of precariousness, insufficient social protection and the issue of algorithmic management.
- **Sustainability and energy efficiency** has to be ensured, on the level of production provisioning of digital services as well as in internet governance (resources needed are still mined under socially and environmentally disastrous conditions; products should come with information on energy consumption in its production process; durability and possibilities of repair and reuse have to be in the focus).
- **Regulations have to be informative and precise** in order to provide a predictable and stable legal framework that allows for innovation to take place.
- **Regulations should aim to enable 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 need to be ensured.
- Alliances under the Important Projects of Common European Interest[8] (IPCEI) and Digital Innovation Hubs for the sharing of knowledge and best practices should be diversified to include more SMEs from peripheral regions of the EU, and their outreach and communication need to be improved.

---

[8] More information: https://ec.europa.eu/competition-policy/state-aid/legislation/modernisation/ipcei_en

## Call to Action:

1. **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.
2. **Introduce corporate tax rules** so that profits are registered and taxed based on where businesses geographically have significant interaction with users through digital channels.
3. **Set up/establish a central pool of advisors** that can be requested by smaller companies to advise them on what can be improved (advocating open source, enabling knowledge sharing, sustainable practices, etc.).
4. **Improve the Market in Crypto-assets (MiCA) regulation**[9] – it must sufficiently differentiate between all crypto asset types to establish a single taxonomy, while also remaining open to new developments; it must be clear which assets fall under its regulation, especially since the lack of regulation of these assets is very problematic, enabling fraud, market manipulation and money laundering, e.g. situations in which authoritarian regimes try to circumvent global sanctions via crypto-assets.

---

[9] More information: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-crypto-assets-1

# ANNEX – GLOSSARY

**TOPIC 1: Digital Democracy** - The use of information and communication technologies (ICT) in political and governance processes.

**E-government** - the use of ICT to enhance public administration or public services.

**E-transparency** - the use of ICT to enhance transparency of governments by allowing citizens to access information online.

**E-participation** - the use of ICT to allow citizens to participate in decision making processes, to improve policy outputs and even co-create policies together with their representatives

**E-voting/E-elections** - to allow voters to record secret ballots and have it tabulated electronically in an election system

**TOPIC 2: Digital Education** - Resetting education and training for the digital age.

**Digital Competencies** - the set of basic digital skills, covering information and data literacy, online communication and collaboration, digital content creation, safety and problem solving

**Digital Skills** - Job related skills: a set of specific digital skills for those involved in jobs including the use and maintenance of digital tools such as 3D printers, CAD software and robots. Digital skills for ICT professionals: a set of advanced, highly specialised, digital skills for those involved in the ICT occupations, for example programmers and cyber security experts who are expected not only to use but also challenge and innovate existing information and communication technologies and create new solutions.

**Digital Learning** - the innovative use of digital tools and technologies during teaching and learning

**Media Literacy** - the skills that allow people to access, critically evaluate, and crate or shape the media

**Awareness Raising** - informing and communicating to citizens about digital practices

**TOPIC 3: Digital Safeguards** - safeguards 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.)

**Cybersecurity -** The protection from hackers, fraud, viruses etc. and managing risks of hybrid attacks - by state and non-state actors - through a mix of cyberattacks, damage to critical infrastructure, disinformation campaigns and radicalisation of the political narratives.

**Artificial Intelligence -** An AI that is ethical and that protects people, communities and society from the escalating economic, political and social issues posed by AI.

**Algorithms -** transparency of algorithms.

**Online Disinformation** - Protection against false, inaccurate, or misleading information used to intentionally cause public harm or make a profit.

**Audiovisual 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. Rules on audiovisual advertising, the promotion of European works, and providers' obligations with regards to the protection of minors from potentially harmful content, among other measures.

**Integrity of Elections** - Rules to ensure greater transparency in the area of sponsored content in a political context (e.g. 'political advertising'); protection of the integrity of elections and promotion democratic participation.

**Terrorist content** - protection against the use of the internet by terrorist networks for spreading their propaganda and recruiting followers.

**Online Hate Speech** - Prevention of practices that denigrates people based on their race, ethnicity, gender, social status, sexual orientation, religion, age, physical or mental disability among others (infringing our rights to freedom of information and to non-discrimination).

**Illegal Content Online -** Measures to effectively tackle illegal content online, including issues such as incitement to terrorism, illegal hate speech, child sexual abuse material, infringements of Intellectual Property rights and consumer protection.

**TOPIC 4 Digital Rights** - Defending Rights & Freedoms Online

**Secure & Sustainable Digital Infrastructures -** The right of everyone to have an access to technological infrastructures.

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

**Digital Services -** The right to fair, transparent and accountable digital services' content moderation processes; ensuring that fundamental rights are respected and guaranteeing independent recourse to judicial redress.
Online Privacy - The level of privacy protection an individual has while connected to the Internet, such as the amount of online security available for personal and financial data, communications, and preferences.

**E-Information** - The right to access information given by governments, companies, etc.

**Net Neutrality** - The right to internet access which should be offered to everyone on a nondiscriminatory basis, without favoring certain websites, applications, or services.

**Data (Protection & Retention) -** the right to data protection and knowledge about data retention.

**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.

**Online Safety of Journalist & Ensuring Plurality of Voices in Digital Media** - The protection of journalists and media workers against the threats to freedom of expression and plurality of information.

**Protecting Fundamental Rights** in the Online Environment.

**TOPIC 5 Digital Economy** - the development of an economy that based on digital computing

**Digital Industry 4.0** - Industry 4.0 is the comprehensive transformation of the whole sphere of industrial production through the merging of digital technology and the internet with conventional industry.

**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.

**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.

**Supporting Green Digital Solutions** - the use of green digital technologies for the benefit of the environment - mainly by deploying and investing more green digital technologies to achieve climate neutrality and accelerate the green and digital transitions in priority sectors in Europe.

**Social Welfare in the Digital Age** - Digital transformation of public welfare services.

**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.).