Council of the
European Union

Brussels, 10 March 2023
(OR. en)

7211/23

LIMITE

CONUN 75
ONU 18
COPS 120
TELECOM 63
CYBER 50
COHOM 69
DEVGEN 53



**NOTE**

| | |
|---|---|
| From: | General Secretariat of the Council |
| To: | Delegations |
| Subject: | European Union Contribution to the Global Digital Compact |

Delegations will find attached the European Union Contribution to the Global Digital Compact, as agreed by the United Nations Working Party on 8 March 2023.

**EUROPEAN UNION CONTRIBUTION TO THE GLOBAL DIGITAL COMPACT**

**INTRODUCTION**

The United Nations General Assembly has decided[1] to hold a 'Summit of the Future' in 2024, aimed, inter alia, to reinvigorate multilateralism, boost implementation of existing commitments, and agree on concrete solutions to challenges. The Global Digital Compact (GLOBAL DIGITAL COMPACT) is expected to be one of the outcomes of the Summit as part of 'Our Common Agenda' representing the UN Secretary-General's vision on the future of global cooperation. The UN Secretary-General's Envoy on Technology coordinates the Global Digital Compact. The UN co-facilitators of the Global Digital Compact are Rwanda and Sweden.

The EU is to submit a contribution to the Global Digital Compact by a single adopted document. The European Union jointly prepared this document in line with international instruments on human rights and in line with the European Declaration on Digital Rights and Principles for the Digital Decade.

The EU expects the Global Digital Compact to be anchored in respect for human rights and serve as a roadmap for a human-centric, global digital transformation. It should be ambitious and express a clear vision that provides a framework for the increasing activity across the UN family, and be anchored in robust support for Human Rights. We expect the Global Digital Compact to support an internet that is open, stable, free, inclusive, global, interoperable, reliable, secure and sustainable.

1 A/RES/76/307

The Tech Envoy has a unique chance to improve coherence and coordination, as well as intra-UN compliance including particularly the ITU, UNESCO, UNIDO and the IGF. The EU considers that the Tech Envoy should play an advocacy role in the global debate on digital, in particular with the general public, putting the emphasis on the different options and scenarios that technology brings about. The Tech Envoy should also uphold and improve the current multi-stakeholder model of internet governance, which is open, inclusive and decentralised. The independent and neutral position of the Tech Envoy, under the direct responsibility of the UN Secretary-General, can also ensure that the promotion and protection of international human rights standards are mainstreamed through all the strands of action of the Roadmap's and Common Agenda's implementation, making clear that the priorities remain profoundly interconnected.



## 1. CONNECT ALL PEOPLE TO THE INTERNET, INCLUDING ALL SCHOOLS

### Core Principles

Some 2.7 billion people in the world lack access to the Internet[2] - the majority of whom are women and girls in low- and middle-income countries. Furthermore, two thirds of the world's school-age children – or 1.3 billion children aged 3 to 17 years old – do not have an Internet connection in their homes.

**Digital connectivity** is essential for working, learning and accessing basic services. Digital connectivity brings people together, keeps us connected, independently of where we are. Broadband connectivity and satellite and cloud technology are a necessity in the transition towards a data-driven economy and society.[3]

2 ITU facts and figures 2022

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

Information and communication technologies (ICTs) can help accelerate progress towards every single one of the 17 United Nations Sustainable Development Goals (SDGs), including SDGs on education and helping to build resilient infrastructure, promoting inclusive and sustainable industrialization, and fostering innovation.

Internet connectivity remains key to ensuring equitable access to the digital sphere for all, including women and young persons, to the digital sphere. Certain groups have specific needs, and therefore require special attention in this context. Connecting all people to the internet should result in accessible, **affordable, inclusive, secure, safe and high quality access, via trusted networks to the open Internet.** As such, indicators to monitor progress and related challenges should be developed for global use.

**Digital transformation** should be based on the **right to interact digitally with public authorities** following a "mobile first" approach as primary authenticator giving the choice to use – wherever practically feasible – mobile devices and mobile digital means to communicate and interact with public services. Alternative options should be provided for users not able to use a mobile phone or a tablet.

The COVID-19 pandemic heightened the importance of access to secure and trustworthy digital infrastructures and technologies, underpinned by **proper regulation** including in the field of health[4]. This includes the protection of users' rights online and the creation of fair, open and contestable online markets. Net neutrality is a key issue to be maintained and protected.

[4] The European Union's Digital Services Act and Digital Markets Act aim to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses.

The **digital transformation of education** could provide unique opportunities to accelerate the achievement of inclusive and equitable quality education (SDG4) and lifelong learning opportunities for all. Quality education is a human right and should be regarded as a public good with particular focus on the most marginalised learners, teachers and parents. For this to happen the global digital divides, including the gender digital divide need to be overcome[5].

As **digital skills often constitute a barrier to internet access**, all persons should be able to acquire the basic and advanced digital skills, including media and information literacy. They need to become well-informed and responsible digital citizens and to be able fully, equally and meaningfully to participate in all spheres of the digital economy and society, and political life. Digital skills are best acquired in the classroom starting from elementary school and developed further on a constant basis throughout the lifetime. Preventing and countering threats, such as online violence and harassment as well as cybersecurity awareness and hygiene must underpin the digital transformation of everyday activities. Every school should be connected to internet services and internet services should be extended to households and individuals in order to provide additional avenues to education and lifelong learning.

**Key commitments**

Helping to achieve a sustainable **digital transformation for everyone in the EU**, the EU has set out concrete targets for digital transformation through the Digital Decade Policy Programme 2030 that evolves around four cardinal points: skills, digital transformation of businesses, secure and sustainable digital infrastructure, and digitalisation of public services, which all may serve as targets for the GLOBAL DIGITAL COMPACT. The success of digital transformation depends on the efficient combination of private investments and public funding instruments. Investments into

[5] Research by UNICEF and ITU has shown that whereas in high-income countries 87 % of children and youth have an internet connection at home, versus 6% in low-income countries.

digital infrastructure are necessary, especially in rural areas and outermost regions. Therefore, we encourage and support substantially investments in 5G and fibre[6].

To maximise the impact of public investment, a **modern regulatory framework** is a precondition. The European Electronic Communications Code now includes essential pro-investment rules, both in spectrum management and in access regulation. Elements of the EU regulatory framework have been adopted in other parts of the world that share the commitment to a human-centric digital and green transformation. For example, the EU supports actions to develop regional roaming agreements and provides technical assistance and expertise. All these actions may serve as indications for the GLOBAL DIGITAL COMPACT.

Everyone has the right to **education, training and lifelong learning** and should be able to acquire basic and advanced digital skills. The EU's Digital Education Plan offers good examples in this aspect. The EU promotes – and expects the Global Digital Compact to promote - access to affordable, stable open, accessible, safe, secure and high-speed internet for higher education, including by investing in connecting schools. The EU commits to support efforts equipping education and training institutions with digital connectivity, infrastructure and tools, in line with the **2022 Transforming Education Summit and the GIGA initiative by UNICEF and ITU** to implement the policies, regulations, technologies and financing required to ensure that school connectivity is safe, sustainable and equitable. The EU is also committed to enable **learners and teachers to acquire and share the necessary digital skills and competences** to take an active part in the economy, society, and in democratic processes. Everyone should have the possibility to adjust to changes brought by the digitalisation of work through up-skilling and re-skilling, in line with the European Declaration on Digital Rights and Principles for the Digital Decade.

[6] To reach the 2030 targets, the EU will, *inter alia*, continue to support the deployment of Gigabit and 5G networks through the Connecting Europe Facility (CEF Digital) with a budget of €2.1 billion over 7 years. CEF Digital *inter alia* supports 5G infrastructure for smart communities, including in rural areas. In addition, the Recovery and Resilience Facility dedicates more than €16 billion to connectivity, including Very High-Capacity Networks and 5G roll-out in remote areas. The EU is also leveraging connectivity investments through the new Cohesion Funds, the EAFRD for regions and InvestEU.

In line with its Global Gateway initiative, the EU invests in the digital world to promote connectivity, peace, and sustainable development and to protect human rights, democracy and the rule of law worldwide. It supports UN agencies and other organisations, including, UNESCO, the Council of Europe and others to ensure that human rights are applied both offline and online. They also underpin the support for the Declaration of the Future of the Internet, which has 70 signatories. The EU works actively in UN fora, including the Human Rights Council and the UN General Assembly Third Committee, to promote global cooperation on digital and human rights.

As a result, including in light of its own commitments, the EU considers that the Global Digital Compact can help achieve consensus around the following areas:

- The importance of an **Internet that is open, stable, free, inclusive, global, interoperable, reliable, secure and green**[7]. Restrictions of and on the Internet threaten global and open cyberspace, as well as the rule of law, human rights and democracy – the core values of the European Union (EU). The EU expects the Global Digital Compact to commit to ensuring access to excellent connectivity for everyone and protecting a neutral and open Internet where content, services, and applications are not unjustifiably blocked or degraded.
- The need to close the various **digital divides**, including digital gender gaps, fostering access to digital, information and media education, and empowering everyone, regardless of age, ethnic or social origin, disability, geographical location, sexual orientation and gender identity or any other status or condition. This is with special regard to those in vulnerable situations so that they may participate confidently and safely in today's digital society and economy. It needs to be ensured that all of the world's people, including those in Least Developed Countries, Landlocked Developed Countries and Small Island Developing States, are able to benefit from the digital transformation and that the rights of persons in vulnerable situations are protected. The EU supports this with considerable resources, alongside sustainable, long-term human capacity building.

7 The twin green & digital transition: How sustainable digital technologies could enable a carbon-neutral EU by 2050

- **Regulatory frameworks** that promote the deployment of digital networks and infrastructures such as submarine and terrestrial fibre-optic cables, mobile wireless systems, space-based secure communication systems as well as cloud and data infrastructures, which together provide a basis for exchanges of data. The EU will work with partners on these topics, and cooperate in high performance computing, Artificial Intelligence (AI), and earth observation. The EU will prioritise underserved regions, countries and populations, including those affected by aggressive and hostile actions, such as Ukraine, supporting the process of rebuilding ICT infrastructure and connections and strengthening secure and trusted digital connections within them and between Europe and the world.

- The need to **minimize the environmental footprint** of digital infrastructure, the internet and digital technologies, by promoting green data centres and supporting the deployment of submarine telecom cables[8] equipped with ocean monitoring sensors that will be put at the service of science (Oceanography, Geophysics, etc.) as well as of the population by contributing to sustainability and mitigating the impact of natural disasters. The EU will ensure that the digital transformation is supported by sufficient clean energy. Global Gateway investments are used to adapt to the needs and strategic interests of different regions, while remaining values-driven.

**Key EU documents**

- European Declaration on Digital Rights and Principles for the Digital Decade
- Decision (EU) 2022/2481 establishing the Digital Decade Policy Programme 2030
- Declaration for the Future of the Internet
- Global Gateway Joint Communication
- DigComp 2.2
- Digital Education Action Plan (2021-2027)

[8] Such as the BELLA Programme between Latin America and Europe or the planned Far North Fiber, pan-arctic submarine cable system, connecting Europe, North America and Asia via the Northwest Passage.

- Digital transformation strategy for Africa 2020-2030.
- European Green Digital Coalition
- EU Action Plan for Human Rights and Democracy 2020-2024
- Multiannual work programme for 2021-2025 - Connecting Europe Facility – Digital



## 2. AVOID INTERNET FRAGMENTATION

### Core principles

The Internet has been conceived and developed as a single, global, decentralised network of networks. Under this model, it has helped connecting people and organisations worldwide and contributed to shape the current economic and social context. All parties should work to ensure that the Internet continues to evolve as an **open network of networks**, a single interconnected communication system for all of humanity.

The EU shares a **vision of the Internet** that is open, stable, free, inclusive, global, interoperable, reliable, secure and green and puts humans and their rights at the centre of digital transformation. The concrete principles to which the EU adheres can be found in the Declaration on European Digital Rights and Principles for the Digital Decade and the Declaration for the Future of the Internet.

The EU vision is:

- To promote the evolution of the current model of the Internet inside the multi-stakeholder and inclusive institutions that develop, deploy, and manage the protocols, standards and core infrastructures of the internet. This will avoid fragmentation on a technical level.
- To protect and fortify the multi-stakeholder ecosystem of Internet governance and keep fundamentals of the Internet out of geopolitics. The EU is committed to engaging in existing

global and regional multi-stakeholder fora (such as the Internet Governance Forum) to discuss and negotiate internet governance issues.This will avoid fragmentation of the governance of the internet.

- To promote a human-centric approach to the Internet. The EU pays specific attention to Digital markets, which need to be open, fair and contestable. The EU also promotes a global digital transition based on affordable, inclusive and reliable access, human rights and fundamental freedoms.

- To avoid commercial or economic fragmentation, which could have an impact on the Internet architecture.
- To ensure that national and international legislation and government practices affecting the internet are designed to promote and protect human rights. This will avoid user experience fragmentation.

**Key commitments**

Reflecting its own commitments, the EU considers that the Global Digital Compact should promote the following commitments, which are required to avid the fragmentation of the Internet:

- Participation in and strengthening of the multi-stakeholder and inclusive system of Internet governance, including the development, deployment, and management of its main technical protocols and other related standards and protocols.
- Given its place as the premier independent forum for multistakeholder input, the EU supports the **Internet Governance Forum** (IGF) and its potential to grow into an always more incisive, inclusive, and sustainable model. The EU also supports the IGF provision of multistakeholder input into the Global Digital Compact.
- Preserve the technical infrastructure essential to the general availability and integrity of the Internet, including by refraining from internet shutdowns or degrading internet access.
- **Put people at the centre of digital transformation** by strengthening the democratic and participatory framework[9], ensuring the protection of and respect for human rights online and offline, fostering responsible and diligent action by all digital actors public and private,

[9] Including a strong judiciary, respect of rule of law, developing strong institutions.

supporting local data and technological ownership as well technological capacity building for a safe and secure digital environment. The EU will actively promote the human-centric centric and green vision of digital transformation, including globally.

- Continue to protect and promote human rights and fundamental freedom online by establishing robust safeguards and defining responsibilities for platforms, especially for **very large online platforms**.

**Key EU documents**

- European Declaration on Digital Rights and Principles for the Digital Decade
- Digital Service Act
- Digital Markets Act
- Council Conclusions on EU Digital Diplomacy
- NIS2 Directive

### 3. PROTECT DATA

**Core Principles**

As explained in the European Declaration on Digital Rights and Principles for the Digital Decade, everyone should have access to safe, secure and privacy-protective digital technologies, products and services. This implies protecting the interests and rights of people, businesses and public institutions against cybercrime, including cyberattacks and data breaches, and confronting those that seek to undermine the security of our online environment. This includes protecting digital identity from identity theft or manipulation. Protection of personal data in the digital domain in the EU is governed by the EU General Data Protection Regulation (GDPR), which is echoed in similar

regulations in the EU Neighbourhood, Africa, Asia and in the Americas. Concerning other types of data, the proposal for an EU Data Act will introduce mandatory safeguards to protect non-personal data of EU customers held on cloud infrastructures against unlawful access by non-EU/EEA authorities.

The European data governance framework– built on the basis of the European strategy for data - aims at **promoting and protecting** human rights and democratic values, and the right to privacy, which is a precondition in all matters related to data access, sharing and use and to data governance, including those related to non-personal data. The principles **empower** individuals and companies with respect to the data they contribute to produce, both personal and non-personal. They control such data and have the right to decide who can access them and for what purposes. Individuals' and companies' sensitive **data** should be protected from unlawful access and transfer requests. Data quality is also a key issue in several areas such as health. Those who seek to undermine **security online** or to promote violence, harassment and hatred through digital means need to be held accountable in ways that adhere to the principles of legality, necessity and proportionality. It is key to ensure the use of quality data and that data collection and methods of use and analysis are inclusive, gender-responsive, ensuring confidentiality and without risk or harm for whose data is collected, and do not reproduce gender bias, stereotypes and discriminatory social norms.

The EU remains committed to the concept of **data free flow with trust**. We believe that there is a need to allow the free flow of data with confidence in order to foster innovation and business opportunities across all sectors, while at the same time recognizing the need for governments to retain the ability to regulate data flows, both for personal and non-personal data, and to address current and future challenges related to cross-border data flows. The EU will work towards ensuring that its businesses can benefit from the international free flow of data in full compliance with EU data protection rules and other public policy objectives, including public security and public order. In particular, the EU will continue to address unjustified obstacles to data flows while preserving its regulatory autonomy in the area of data protection and privacy.



**Key commitments:**

The EU promotes internationally a **data governance model**, based on a human-centric and values-based approach and taking into account the importance of cross-border data flows for EU businesses, in order to develop digital partnerships and to organise international data flows by guaranteeing the outmost respect and promotion for human rights and values.

The EU therefore expects the Global Digital Compact to have a strong focus on the protection of personal and non-personal data.

- While the GDPR provides a set of standardized data protection laws throughout the EU, an important component of privacy and human rights law, the EU will contribute to the creation of a legal framework in which data of EU citizens and companies are protected, also in the context of **international data transfers**. The shielding provisions established in the Data Governance Act for sensitive publicly held non-personal data, and proposed in the Data Act also for cloud and edge services, are available as examples.

- Concerning other types of data, the proposal for an EU Data Act will introduce mandatory safeguards to protect non-personal data of EU customers held on cloud infrastructures against unlawful access by non-EU/EEAS authorities. The proposal will ensure fairness in the data economy, stimulate competitiveness of European business and open opportunities for data-driven innovation.

- The EU helps develop regulatory frameworks that prevent the establishment of a data-extractive model globally, and in particular in emerging markets, and is ready to support the development of such frameworks.

**Key EU documents**

- European Declaration on Digital Rights and Principles for the Digital Decade
- Global Gateway Joint Communication
- EU Data Act
- EU Data Governance Act:
- EU General Data Protection Regulation (GDPR)
- Data Quality Framework for EU medicines regulation
- Good practice guide for the use of the Metadata Catalogue of Real-World Data Sources
- European Data Strategy

## 4. APPLY HUMAN RIGHTS ONLINE

### Core principles

Digital technologies have vastly improved the way we communicate, engage and consume and contribute to the respect and enjoyment of human rights, including, freedom of opinion and expression, freedom of association and assembly, freedom of religion or belief and access to trustworthy information. New technologies have a key role in facilitating the documentation of violations of international human rights and humanitarian law violations as well as war crimes. Emerging new technologies can also be instrumental in facilitating access to health, employment, information, participation, education and many other areas. However, these technologies can also have a negative impact, such as more widely spreading disinformation and hate speech, enabling new forms of violence, violations and abuses of the right to privacy, facilitating access to specific illegal content including child sexual abuse and exploitation, widespread surveillance limiting freedom of expression and reducing civil society space, reinforcing discrimination and structural inequalities.

Human rights apply both online and offline. The same rights that humans enjoy offline, civil and political rights, as well as, economic, social or cultural rights, must also be promoted and protected online.

Digital technologies must be human-centred and human rights compliant. New technologies can contribute significantly to the protection and promotion of human rights, democracy and gender equality including by making public participation easier and more effective, increasing access to public services, facilitating the documentation of violations and abuses of human rights, and fostering online activism.

A human rights-based approach is at the core of the EU´s human-centric vision for the technological transformation, which is based on the promotion and protection of the rule of law, human rights and democracy. A human rights-based approach to the whole life-cycle – i.e. the design, development, deployment evaluation and use – of digital technologies puts human rights at the centre of all considerations and actions related to existing and emerging challenges.

To affirm its commitment to applying human rights online, the European Union adopted new standard-setting rules that aim to create a safer and more trustworthy online space for users and consumers. The Digital Services Act (DSA) provides users with new tools to better exert their rights, and defines clear responsibilities and obligations for online platforms. For example, very large online platforms will now be obliged to assess and mitigate the risks posed by their systems, including to the protection of fundamental rights, public interests, public health and safety, and to subject their assessments and measures to an independent audit.

In establishing rules and obligations, the DSA has a particular focus on addressing the impact of digital technologies on persons in vulnerable situations, and on ensuring gender equality and non-discrimination. In addition, special attention needs to be paid to the rights of children and youth, as there is a significant

The DSA seeks to enhance freedom of expression online, make marketplaces safer and address illegal content and societal risks to the benefit of both consumers and companies, ensuring that we do not have to face a trade-off between the safety of our citizens and the freedom of expression online. Under the DSA, companies providing digital services are responsible for ensuring users' safety and trust and guaranteeing respect for human rights in a transparent manner. At the same time, the DSA prohibits, EU governments from forcing digital services to engage in general monitoring. These new rules will complement and harmonise the work done to tackle different types of illegal content.

Children face particular issues online, including exposure to violence and harm, inter alia sexual exploitation and abuse, technology-facilitated solicitation, cyberbullying, cyber harassment, cyber procuring, human trafficking, information manipulation and interference, as well as breach of their right to privacy and their right to be forgotten. Children have the fundamental right to have their best interests assessed and taken into account as a primary consideration in all decision and actions that affect them. The fight against child sexual abuse is of high priority for the European Union. This crime knows no borders and requires a comprehensive, multi-stakeholder and global approach and effective tools. Targeted and robust prevention plays a key role in protecting children against child sexual abuse and sexual exploitation.  The provisions on the protection of minors in the DSA

reaffirm that a safer and better digital environment for children and young people is a key priority for the European Union. The recently updated EU Better Internet for Kids strategy (BIK+) contributes to the implementation of the regulatory framework, in particular the DSA.

The European Commission uses dedicated funding to support, effective prevention initiatives targeting perpetrators and persons at elevated risk of committing offences against children, including online. It also supports technical tools for law enforcement to develop the capabilities of units dedicated to investigating crimes of child sexual abuse and exploitation more efficiently while fully guaranteeing privacy and the protection of personal data. At the global level, the Commission works closely with a number of key stakeholders, in particular the WeProtect Global Alliance to eradicate online child sexual abuse (WPGA), to contribute to the development of global standards to protect children from these crimes and promote awareness and multi-stakeholder cooperation.

While technological change and digitalisation can accelerate progress for gender equality and the empowerment of all women and girls, they can also exacerbate vulnerability, existing inequalities, gender stereotypes and discriminatory social norms with serious risks and implications for women and girls in particular. Incitement to hatred and violence, and all forms of online sexual and gender-based violence as well as disinformation are spreading, often disproportionately affecting women and girls. This is an opportune moment for the international community to make bold commitments to step up action at the national, regional and international levels to ensure that innovation, technological change and digital education will accelerate gender equality, whilst preventing, mitigating and managing all potential harmful impacts.

There is a pressing need for the world to present a united front and commit to an open, stable, free, global, inclusive, interoperable, reliable, secure, and green Internet. This should be accompanied by efforts to ensure a safer and more transparent digital environment, where human rights are protected and no one is discriminated against based on sex, race, ethnic, national or social origin, religion or belief, political or any other opinion, disability, age, sexual orientation and gender identity or any other ground.

The European Union is firmly committed to a vision of the Internet as a safe and trusted space for everyone, where the fundamental freedoms and human rights we promote, protect, enjoy and apply offline, are also protected, promoted enjoyed and applied online. The EU believes that digital technologies have the potential to promote and reinforce democracy, peace and human rights, as described in the Universal Declaration of Human Rights, as well as the principles of the rule of law, legitimate purpose, non-arbitrariness, effective oversight, and transparency.

While necessary and appropriate regulation is incumbent on governments in accordance with their human rights obligations, addressing the impact of digital technologies on human rights requires a multi-stakeholder approach to policy-making, involving national authorities, national human rights institutions, academia, civil society, human rights defenders, journalists, international and regional organizations and the private sector.

The Terrorist Content Online (TCO) Regulation, which entered into application on 7 June 2022, has also uniform rules to ensure terrorist content aimed at spreading propaganda, providing instructions, recruiting followers, and facilitating and directing terrorist activities, is removed within one hour after receiving a removal order by an EU Member State. In particular, it regulates the duties of care to be applied by hosting service providers (HSPs) as well as the measures to be in place on the part of Member State' authorities in order to identify and ensure the quick removal of terrorist content online and to facilitate cooperation between Member States and Europol.

**Key commitments**

The EU expects the Global Digital Compact to promote a human rights-based approach to the whole cycle of digital technologies – including design, development, deployment, evaluation and use – as part of a coherent narrative of the human-centric vision of the digital transformation, including in international standard-setting processes. The EU is committed, and expect the Global Digital Compact to commit to ensuring a safe, secure and fair online environment, that facilitates innovation and in which human rights are protected and promoted, and responsibilities of platforms, especially very large online platforms, are well defined.

Co-regulation of the digital space should reinforce the rule of law that is essential to well-functioning democracies. Through the combined regulatory package of the Digital Services Act (DSA) and the Digital Markets Act (DMA), the European Union is taking a systemic approach to set global standards for online platform regulation, which optimises the balancing of the different human rights online. The EU supports the work done on this by UNESCO and would welcome its inclusion in the GLOBAL DIGITAL COMPACT. Anti-corruption, media and information literacy, election integrity and other capacity-building efforts are additional elements required to build resilient societies.

The EU is committed to, and expects the Global Digital Compact to support an online environment where people are safe from information manipulation, online sexual and gender-based violence and harassment and interference, including hate speech and other forms of harmful content, such as Child Sexual Abuse Material (CSAM) and/or disinformation. The Global Digital Compact should equally address the problems of Terrorist Content Online, including removal of online content.

In line with the EU Action Plan on Human Rights and Democracy 2020-2024, promoting human rights and democracy in the use of digital technologies, including artificial intelligence, is one of the main priorities of EU external human rights policy. The EU expects the Global Digital Compact to promote the rights to privacy and data protection, addressing arbitrary and mass surveillance and **actively combating internet shutdowns (and misuse of the internet, e.g. for arbitrary surveillance of civil society actors and spaces)**, online censorship, hate speech online, online

sexual and gender-based violence, information manipulation and interference, including disinformation and cybercrime, in full compliance with international human rights law. Through its policies to support human rights defenders (HRDs), the EU will continue to fund trainings in digital security for civil society, journalists and human rights defenders and to fund emergency measures to protect HRDs in the online sphere. The EU will continue to pay particular attention to categories of HRDs particularly at risk such as women human rights defenders, LGBTI rights defenders, and defenders of land, environmental and indigenous peoples' rights.

During the last decade, several EU laws have been adopted in different areas to make the EU more digitally accessible for persons with disabilities, among others the Web Accessibility Directive, which requires websites and mobile applications of public sector bodies to be digitally accessible, the European Accessibility Act covering also many private sector products and services, and the

European Communications Code covering accessible emergency communications. It should be noted that while digital accessibility features are essential for some, they are often useful for all users.

With the **European Declaration on Digital Rights and Principles for the Digital Decade**, the European Union spells out how values and human rights should be applied in the online world. The Declaration refers to EU law, from the Treaties to the Charter of Fundamental rights but also the case law of the Court of Justice. It builds on the experience of the European Pillar of Social Rights. This vision, which can be reflected in the GLOBAL DIGITAL COMPACT, includes: putting people at the centre of the digital transformation; underlying solidarity and inclusion; restating the importance of freedom of choice; participation in the digital public space; safety, security and empowerment; and sustainability.

These principles should accompany people in their everyday life: accessible, affordable and high-speed digital connectivity everywhere and for everybody, well-equipped classrooms and digitally skilled teachers, seamless access to public services, a safe digital environment for everyone, disconnecting after working hours, obtaining easy-to-understand information on the environmental impact of our digital products, controlling how their personal data are used and with whom they are

shared. to combat all forms of discrimination, with a specific attention to multiple and intersecting forms of discrimination, including on grounds of sex, race, ethnic or social origin, religion or belief, political or any other opinion, disability, age, sexual orientation and gender identity.

At international level, this commitment to a human rights-based approach has taken the form of the **Declaration for the Future of the Internet (DFI)**, which promotes an affirmative, positive and strategic agenda for a free, open, global, interoperable, reliable, and secure Internet, and commits to strengthen our work to combat violence online. The DFI convincingly builds on universally agreed digital rights and principles as a standard for the entire world.



**Key EU documents**

- European Declaration on Digital Rights and Principles for the Digital Decade
- Digital Services Act
- Digital Markets Act
- EU Action Plan on Human Rights and Democracy

## 5. INTRODUCE ACCOUNTABILITY CRITERIA FOR DISCRIMINATION AND MISLEADING CONTENT

**Core principles**

**Digital ecosystems should be based on transparency and ensure free flow and wide availability of high-quality and pluralistic information**, empowering citizens against information manipulation and interference, including disinformation, discrimination online gender-based violence and harassment and misleading content online, while ensuring an **open, stable, free, global, inclusive, interoperable, reliable, secure, and green Internet** and fully respecting **human rights, democracy and the rule of law**. The recent Declaration on Digital Rights and Principles recalls most relevant rights in this respect.

Everyone, regardless of their age, gender, abilities, condition, or geographical location, has a right to **benefit fully from safe, secure and fair online environment**, where human rights are protected and promoted, and responsibilities of government, platforms and other tech actors are well defined.

The **transparency regarding the origin of information** and the way it is produced, sponsored, used, disseminated and targeted should be improved.

Citizens should be **empowered to make their own, informed choices online**, based on access to diverse, transparent, reliable and easily accessible information, and **equipped with information and media literacy skills** they need to **defend themselves against discriminatory, violent, false or misleading content**, manipulated information and disinformation, which used to violate and erode human rights, deepen inequalities, spread dangerous misinformation and fuel discrimination, xenophobia, misogyny and racism.

Stakeholders should **address challenges presented by online** disinformation, information manipulation and interference, which can erode public trust in democratic processes and institutions, as well as the citizens' exercise of their sovereign power free of foreign interference and incite discrimination, intolerance and violence, including online gender-based violence and harassment. Any limitations to freedom of expression must remain within strictly defined parameters flowing from international human rights law, such as legality/legitimate interest, necessity and proportionality.

**Inclusive solutions** should be promoted through awareness-raising, media and information literacy, broad stakeholder involvement and the cooperation of public authorities, platforms, media and other online actors, as well as civil society. In order to make governmental services more inclusive and more accessible, the "mobile first" approach should be applied where possible supplemented by alternative authentication options for users not able to use a mobile phone or a tablet.

**Key commitments**

Reflecting its own commitments, the EU considers that the Global Digital Compact should promote the following principles and actions to ensure transparency and accountability:

- **Strengthen multilateral and multi-stakeholder engagement** to tackle discriminatory content as well as false and misleading content at all levels, notably within the United Nations and with other international and regional organisations, to advocate transparent and accountable content

governance frameworks that protect freedom of expression and enhance the availability of accurate and reliable information in the public sphere, while fully respecting human rights, democracy and the rule of law.

- **Strengthen cooperation of public authorities', platforms and other tech actors media and civil society** to protect individuals against information manipulation and interference, including disinformation and other forms of harmful content, prevent the rise of hatred online, by developing counter-narratives and measures promoting non-discrimination, tolerance and respect, including through awareness-raising and public communication activities. , as well as addressing the root causes of inequalities, such as discriminatory structures, social norms and gender stereotypes.

- **Strengthen cooperation of public authorities', platforms and other tech actors, media and civil society** to combat gendered disinformation, the spread of gendered misinformation and online sexual and gender-based violence and harassment.

- **Develop international principles on information manipulation and interference, including disinformation** (through, for example, codes of practices) with clear commitments and specific measures, allowing for stronger joint action and accountability, subject to regular monitoring. Signatories could voluntarily commit to take action in several domains, such as demonetising the dissemination of disinformation; ensuring the transparency of political advertising; algorithmic transparency, empowering users to assess the reliability of sources of online content; enhancing the integration of fact-checking by platforms in their services; cooperation with fact-checkers; and providing researchers better access to data.

- **Promote adequate changes in platforms' conduct, aimed at a more accountable information ecosystem**, with increased transparency, enhanced fact-checking capabilities and collective knowledge on information manipulation and interference, including disinformation and discrimination online, and the use of new technologies to improve the way information is produced and disseminated online. Platforms should mitigate the risks stemming from the use of their services, protect freedom of expression and promote free democratic debate online and be held accountable for doing so.

- **Support cooperation and knowledge sharing on standard** setting, policy-making and policy implementation, encourage information sharing to help governmental and non-governmental stakeholders address information manipulation and interference, including disinformation and other harmful content through human rights compatible policies.

- **Share best practices in the UN context**, such as some of those resulting from the **EU Digital Services Act** (DSA), which aims to create a transparent and safe online space to safeguard users against illegal content, online discrimination, and cyber incidents. The DSA is expected to facilitate innovation by digital businesses in the online environment whilst ensuring the protection of fundamental rights, including the principle of consumer protection.

- **Promote digital literacy and life-long development of digital competences**, crucial to reinforce the resilience of our societies to information manipulation and interference, including disinformation and raise awareness of potential issues related to ethics, data protection and privacy, rights of the child, discrimination and bias, including gender bias and disability and ethnic and racial discrimination.

- **Support reliable sources of information and quality journalism.** Public authorities, platforms, media and other online actors as well as civil society should foster exposure to diverse cultural and multilingual, information, and media content in order to contribute to pluralistic public discourse, strengthen inclusion, and bolster resilience to information manipulation and interference, including disinformation.

- **Support** media freedom and protect/ensure journalists' safety online. Freedom of expression and the right not to be subjected to hate speech, incitement to violence etc. as for example reflected in The Rabat Plan of Action and the Santa Clara Principles need to be observed respecting international human rights standards.

- Public authorities and private actors should **refrain from using the Internet to undermine the democratic electoral infrastructure, elections and political processes**, including through covert information manipulation campaigns.

- **Safeguard global security** in the context of countering foreign information manipulation and interference (FIMI), including state-sponsored interference, as well as combatting violence and hate speech, including through support for the **Paris and Christchurch Calls.**

- **Foster greater exposure to diverse quality cultural and multilingual content**, information, and news online. Exposure to diverse content online should contribute to pluralistic public discourse, foster greater social and digital inclusion within society, bolster resilience to information manipulation and interference, including disinformation, and increase inclusive participation in democratic processes.

**Key EU documents**

- Council Conclusions on EU Digital Diplomacy 18 July 2022
- European Declaration on Digital Rights and Principles for the Digital Decade
- Digital Services Act
- Communication on 'tackling online disinformation: a European approach' (2018)
- Action plan on disinformation
- The EU Code of conduct on countering illegal hate speech online (2018):
- European Democracy Action Plan
- The Strengthened EU Code of Practice on Disinformation (16 June 2022)
- Council Conclusions on Foreign Information Manipulation and Interference (FIMI)

## 6. PROMOTE REGULATION OF ARTIFICIAL INTELLIGENCE

### Core principles

In 2018, the global business value derived from Artificial Intelligence (AI) amounted to USD 1.2 trillion. Post-Covid, the use of AI will likely generate three times that: namely USD 4 trillion benefit for global markets[10].

As AI is expanding, the European Union is guided by a **human-centric and pro-innovation approach, to AI based on fundamental rights, and Union values such as democracy and the rule of law, as enshrined recently in the Declaration on Digital Rights and Principles.** For the EU, fundamental rights form the bedrock and are at the centre of all considerations related to existing and emerging challenges and for all regulations and measures concerning the entire lifecycle of new and emerging technologies. Trust and transparency in AI systems are crucial for their acceptance and sustainability. Human oversight, transparency, risk management are the core principles by which to regulate tech business models and their applications.

From the beginning, the European Commission's approach to AI has had the twin objective of creating ecosystems of excellence and trust to promote the development and uptake of AI while addressing the risks associated with certain uses of this technology. The EU **Coordinated Plan on AI** translated these objectives into a set of concrete actions to be implemented by the Commission and Member States. The EU wants AI to be trustworthy, transparent and accountable so that people can trust that the technology is developed, deployed and used in a way which meets a high level of protection of public interests, such as health, safety and the protection of fundamental rights. The **Artificial Intelligence Act** will make sure that Europeans can trust what AI has to offer. Proportionate and flexible rules address the specific risks posed by AI systems, will foster innovation and create legal certainty. The new rules will be applied directly in the same way across all Member States based, on a future-proof definition of AI, and a risk-based approach: systems considered high-risk will have to comply with a number of requirements before being put or being

[10] Roadmap for Digital Cooperation, June 2020, Report of the Secretary-General UN.

used in the EU market. The AI Act is designed to be future-proof: it will include flexible mechanisms that allow the high-risk use cases to be dynamically adapted as the technology evolves. On 28 September 2022, the Commission delivered on the objectives of the White Paper and on the European Parliament's request with the Proposal for an Artificial Intelligence Liability Directive (AILD).

Artificial Intelligence (AI) has become an area of strategic importance and a key driver of economic progress, hence women have to be part of its development as researchers, programmers and users. While AI can bring solutions to many societal challenges, it risks intensifying inequalities and discrimination. Algorithms and related machine-learning, if not transparent and robust enough, risk repeating, amplifying or contributing to unfair biases that programmers may not be aware of or that are the result of specific data selection.

**Key commitments**

In April 2021 the European Commission presented a proposal[11] for a legal framework for AI (AI Act). The Commission proposal puts forward rules for the development, placing on the market and use of AI systems in the EU following a proportionate risk-based approach. It adopts the following topography:

- A limited set of uses of AI that contravene fundamental values or violate fundamental rights are proposed to be **prohibited**: AI systems that distort a person's behaviour through subliminal techniques or by exploiting specific vulnerabilities in ways that cause or are likely to cause physical or psychological harm; general social scoring carried out by public authorities; "real-life" remote biometric identification in public accessible spaces for law enforcement purposes (with some targeted exceptions).
- **High-risk AI systems, posing significant risks to fundamental rights or safety,** must comply with certain requirements which include the use of high-quality datasets (in order to avoid bias and unlawful discrimination), appropriate documentation and information obligations to enhance traceability, transparency, the design and implementation of appropriate human

[11] It is likely to be adopted approximatively by the end of 2023 - beginning of 2024

oversight measures, and the achievement of the highest standards in terms of robustness, safety, cybersecurity and accuracy.

- **Transparency obligations are introduced for certain AI systems:** when using AI systems such as chatbots, deepfakes, emotion recognition or biometric categorisation systems, users should be aware that they are interacting with a machine so they can take an informed decision to continue or step back.
- For **low-risk AI systems**, codes of conducts are encouraged and could be facilitated by the European Commission and the Member States.



In addition, the **Digital Services Act** provides for transparency obligations as regards the terms and conditions of intermediary services, algorithms and recommender systems used by online platforms. Very large online platforms are requested to assess the systemic risks stemming from the functioning of their services and take measures against such risks, including adapting their algorithms, content moderation or recommender systems. The Digital Services Act also provides for the obligation for very large online platforms to give access to their data, including algorithmic systems, to Member States and to researchers.

The EU will continue promoting a, human-centric and balanced approach to AI within the Single Market and globally, covering the whole life-cycle of digital technologies - including design, development, deployment, evaluation and use. It will also continue cooperation at the international level, bilaterally and within the framework of multilateral fora to achieve better coordination, collaboration and governance. The EU expects this approach to be reflected in the Global Digital Compact.

In such fora, the EU will actively engage and participate in **AI discussions**, including on **research and innovation cooperation** as well as **competitiveness**. It strongly believes that ethically applied AI and technology at large can be used to help achieve the **Paris Climate agreement** and the **Sustainable Development Goals (SDGs),** in line with **UNESCO's Recommendation on the Ethics of AI**. Innovative and tested digital solutions may promote efficiency of public administration, public participation in decision-making, and creation of new economic opportunities.

Regarding emerging challenges related to lethal autonomous weapons systems (LAWS), the EU emphasises that human beings must make the decisions with regard to the use of lethal force, exert

control over weapons systems that they use and remain accountable for decisions over the use of force in order to ensure compliance with International Law, in particular International Humanitarian Law. The EU expects these issues on LAWS to be reflected in the Global Digital Compact– in line also with the UNESCO Recommendations on the ethics of AI.

The EU and UNESCO Member States have signed up to the UNESCO recommendations on ethics of artificial intelligence and held the Global Forum on the Ethics of the Artificial Intelligence in Prague on 13 December 2022. The EU, the Council of Europe member states and third countries sharing the same values are currently discussing a Council of Europe Convention on artificial intelligence based on the Council of Europe's standards on human rights, democracy and the rule of law, and conducive to innovation, in accordance with the relevant decisions of the Committee of Ministers[12].

**Key EU documents**

- European Commission (2022): European Declaration on Digital Rights and Principles for the Digital Decade
- United Nations (2021) Our Common Agenda report (commitment No 7 'Improve digital cooperation')
- European Commission (2021): Proposal for a regulation laying down harmonised rules on artificial intelligence COM(2021) 206 final
- European Commission (2021): Coordinated Plan on Artificial Intelligence 2021 Review COM(2021) 205 final
- European Commission (2020): White Paper on artificial intelligence – A European approach to excellence and trust (COM(2020) 65 final)

12 Convention on the design, development, and application of artificial intelligence systems based on the Council of Europe's standards on human rights, democracy and the rule of law, and conducive to innovation, in accordance with the relevant decisions of the Committee of Ministers

- EU High-Level Expert Group on AI (2019): Ethics guidelines for trustworthy AI
- European Commission (2018): Coordinated Plan on Artificial Intelligence (COM(2018) 795 final)
- Council Decision (EU) 2022/2349: Council Decision authorising the opening of negotiations on behalf of the European Union for a Council of Europe convention on artificial intelligence, human rights, democracy and the rule of law
- European Commission (2018): Communication on AI for Europe (COM(2018) 237 final)
- European Commission (2018): "Artificial Intelligence for Europe" (The European AI Strategy)

## 7. DIGITAL COMMONS AS A GLOBAL PUBLIC GOOD

**Core principles**

Digital commons can be defined as information and knowledge resources that are collectively created and owned or shared among a community. With the precondition that contributions and governance be distributed and not centralized in the hands of one or a few entities only, most of the open source software, hardware, standards and open data can be included in this definition.

As reflected in the UN´s Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation - Report of the Secretary-General, the EU considers Digital Public Goods (DPGs) - such as Open Source Software, open data, open standards, AI libraries/standards (open), open content, etc. - as **accelerators of the SDGs** and a contribution to a more equitable world[13].

[13] Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation - Report of the Secretary-General

Digital commons bridge geographical divisions: the commons developed in one area of the world can be re-used or enriched elsewhere, including in developing countries through government agencies, non-governmental organisations, universities etc. These benefits can be translated in economic terms[14], including for the public sector resulting in lower costs and increasing its digital autonomy. Digital commons need to be relevant, safe and sustainable.

**DPGs have to follow certain principles and standards** as also underlined in the UN´s Road map: "In particular, it is fundamental that DPGs be compliant with privacy, digital public rights and a human-centric approach.

The EU supports Digital Public Goods also outside the Union. Due to its participatory nature (the development of DGPs also implies the contribution of the consumers, citizens, academia among others) and knowledge sharing, innovation can be leveraged as well as a stronger competitive market, boosting innovation. DPG Platforms can provide an important contribution to share digital public goods, engage talent, and pool data sets.

Core principles include:

- Encourage talents to contribute to digital commons, including through public funding at national, regional and global levels.
- Facilitate global cooperation of commoners, as commons know no borders.
- Facilitate the interoperability of international Digital Public Goods on the basis of the respect of global core principles and standards.
- Stimulate shared governance of digital commons and avoid concentration.
- Incentivise commoners to develop trust technologies for ensuring transparency, privacy protection, user control and choice through interoperable and standardised commons.
- Enable open data and develop policies to empower more actors – ideally the general public – to use data.

[14] The European Commission published a study in 2021 predicting that an increase of 10% in contributions to open source software code would generate annually an additional 0.4% to 0.6% of GDP, as well as more than 600 additional ICT start-ups in the EU.

**Key commitments**

The European Union has embraced a human-centric approach to digital transformation, where digital technologies, in particular internet technologies, are developed in response to humans' needs and based on the principles of openness, trustworthiness, decentralisation, safety (the key references are the EU Declaration on Digital Principles and Rights and the Declaration for the Future of the Internet).

As reflected in the UN´s Road map for digital cooperation and the SDGs, including SDG 9, and in line with the EU's Global Gateway strategy, the **EU commits to promote and support resilient and trusted digital infrastructures**, the enhancement of democratic digital societies beyond EU borders, digital public infrastructure and **digital public goods, and digital commons**[15]. The European Union is leading several funding and legislative programmes that nurture digital commons, such as:

- **Next Generation Internet initiative:** The European Commission-lead programme provides funding for Open Source software and hardware to more than 700 grass-root projects covering all layers of the Internet, including applications, networks and cloud, which are crucial to develop digital commons and address specific needs of commoners.
- **Data Legislation**: the European Union is actively contributing to the creation of data commons. This effort includes: the Open Data Directive stimulates releasing open government data and open access for research data; the Data Governance Act that intends to reinforce trust in data sharing.
- **Open Source Observatory:** works as a single information point for Open Source initiatives in the EU public sector. It provides Free and Open Source software expertise and information as well as serves as middle-ground to connect European Public Administrations with other relevant stakeholders.
- **Open Source Programme Office (OSPO)**: has been established to promote the role of Public administrations in stimulating general adoption of open source.

[15] Council Conclusions on EU Digital Diplomacy

The EU also supports trust and distribution of digital commons and more broadly digital public goods within broader initiatives, which could also be referenced in the GLOBAL DIGITAL COMPACT:

- Envisaged promotion of DPGs through a collaboration with the International telecommunications Union (ITU) and the United Nations Development Programme (UNDP). This potential action will support 'Open Source Software ecosystem enablers for public service'.

- Acknowledging the work of the Digital Public Good Alliance (DPGA). Member-organisations demonstrate a strong commitment to digital public goods and are committed to supporting the DPGA's mission and mandate.

- The GovStack Initiative: ITU, Estonia, Germany, and the Digital Impact Alliance (at the United Nations Foundation) launched the GovStack Initiative in 2020 with the goal of accelerating national digital transformation and the digitalization of government services for achievement of Sustainable Development Goals by 2030. The Digital Nations work as an international forum of leading digital governments, connected by the principle of user needs, open standards, open source, open markets, open government, connectivity, teaching children to code, assisted digital and a commitment to share and learn.

- The implementation of the recommendations made by nineteen Member States in the report 'Towards a Sovereign Digital Infrastructure of Commons". Under the right conditions, digital commons contribute to the preservation of the collective control and valuation of both quality and re-use of data and digital infrastructures, and consequently foster innovation, social value and sustainability.

**Key EU documents**

- Council Conclusions on Digital Diplomacy
- Our Common Agenda report
- Joint Communication to the European Parliament and the Council on strengthening the EU's contribution to rules-based multilateralism EEAS Website (europa.eu)
- Study on the impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy
- EU Declaration on Digital Rights and Principles for the Digital Decade
- European Commission's Open Source Programme Office plan
- European legislation on open data
- European Data Governance Act
- Data Act
- Next Generation Internet initiative
- Towards a Sovereign Digital Infrastructure

## 8. TRUSTED CONNECTIVITY

### CORE PRINCIPLES

The COVID-19 pandemic heightened the importance of access to secure and trustworthy digital infrastructures and technologies underpinned by proper regulation. As global internet traffic is expected to grow more than six-fold by 2030, broadband connectivity will become a necessity in the transition toward a data-driven economy and society. We recognize the rising energy and resource demands of the increasing use of digital technologies and services, such as data centres and telecommunications networks, and the environmental impacts of production, use and disposal of digital equipment and devices.

Trusted connectivity relies on both physical infrastructure – such as fibre optic cables – as well as an enabling environment that is accessible and affordable, and people have the relevant digital skills. It is important to make sure projects deliver, based on attractive investment and business-friendly trading conditions, regulatory convergence, standardisation, supply chain integration, and financial services.

Investments in connectivity should be human-rights centred and values-based, as well as fully aligned with the UN's 2030 Agenda and its Sustainable Development Goals (SDGs), and the Paris Agreement. Core principles for all EU connectivity investments include:

- Democratic values and high standards
- Good Governance and Transparency
- Equal partnerships
- Green and clean[16]

16 The twin green & digital transition: How sustainable digital technologies could enable a carbon-neutral EU by 2050

- Security-focus
- Catalysing private sector investment
- Human rights and gender equality
- Furthermore, the promotion of digital humanities and digital humanism is essential in this context.

**Key commitments**

In line with the **Global Gateway strategy**, the EU will promote and support resilient and trusted Digital infrastructures, the enhancement of democratic digital societies beyond EU Borders, digital public infrastructure and digital public goods, and digital commons. The EU will offer its financing under fair and favourable terms in order to limit the risk of debt distress. It will help build sustainable infrastructure with the support, skills and the finance needed to operate it. In implementing Global Gateway, the EU will work closely through a Team Europe approach and with like-minded partners to develop synergies between their respective efforts on connectivity and quality infrastructure with third countries and achieve the maximum impact in closing the global infrastructure gap.

The EU will build on the global trend towards convergence with the General Data Protection Regulation (GDPR) to inspire other countries to promote secure data flows. Global Gateway will promote a regulatory model of open and competitive markets for communications networks and services, based on access to the Open Internet, given its role as a key driver of innovation, socio-political, economic, and cultural development.

Reflecting these commitments, the EU considers that the Global Digital Compact should promote the following principles and actions to underpin Trust in the Digital Ecosystem:

- General trust in the digital ecosystem and public institutions as such should be increased through clear democratic principles and institutional initiatives focusing on responsibility,

transparency and human rights. These principles, when implementing specific digital services, may also aid in generating situational trust in public servants and institutions.

- Work together to combat cybercrime, and deter malicious cyber activity, including through multilateral channels. The ongoing work of the *hoc* Committee to Elaborate a Convention on Cybercrime should be supported.
- Work together to combat online hate speech, disinformation and online sexual and gender-based violence and harassment, which widens the gender digital divide, prevents a full, safe and inclusive participation in online spaces and equal participation in society.
- Promote efforts by relevant bodies such as UNODC to support Member States in building up capacities to prevent and combat cybercrime in a holistic manner, including by increasing efficiencies in the investigation and prosecution of cybercrime.
- Promote the protection of consumers, in particular vulnerable consumers, from online scams and other unfair practices online and from dangerous and unsafe products sold online.
- Ensure that government and relevant authorities' access to personal data is based in law and conducted in accordance with international human rights law.
- Protect individuals' privacy, their personal data, the confidentiality and end-to-end encryption of electronic communications and information on end-users' electronic devices, consistent with the protection of public safety and applicable domestic EU, and international law.
- Promote and use trustworthy network infrastructure and services suppliers, relying on risk-based assessments that include technical and non-technical factors for network security.
- Refrain from using the Internet to undermine the electoral infrastructure, electoral and political processes, including through information manipulation campaigns.
- Promote the access to a quality information environment and the exercise of democratic rights[17] free from malicious and inauthentic interference.
- Support a rules-based global digital economy which fosters trade and contestable and innovation.

[17] E.g. freedom of expression, the right to seek, receive and impart information, the right to free assembly

- Cooperate to maximize the enabling effects of technology for combatting climate change and protecting the environment, whilst reducing as much as possible the environmental footprint of the Internet and digital technologies (Green and Digital transition).

**Key EU documents**

- Joint Communication on Global Gateway
- Council Conclusions on Digital Diplomacy
- G20 Principles for Quality Infrastructure Investment (other documents)