ETNO contribution to consultation on UN Global Digital Compact

The European Telecommunications Network Operators' Association (ETNO) represents the telecoms network operators in Europe. ETNO members represent over 68% of the investment into Europe's telecoms networks, the fixed and wireless connectivity which underpins our economy and society, and which is driving the twin green and digital transition.

ETNO has long been involved in global digital leadership, playing a key role at the Internet Governance Forum (IGF) and engaging with the International Telecommunication Union, Council of Europe, and the institutions of the European Union.

Section 1 – general comments

ETNO strongly welcomes the initiative of the United Nations and the Secretary General to propose a Global Digital Compact, as a key high-level track of the Summit of the Future, which recognises the vital role which digital technology and the internet plays in the economy and society of the future. Already today, digital technologies are driving the transition to a more sustainable society.

We strongly support the adoption and signing by many countries of the **Declaration for the Future of the Internet**. The Declaration sets out a positive and ambitious vision, which views the internet and digital technologies as a powerful enabler of positive change, including for combatting climate change, supporting economic growth in the context of a global digital economy which fosters trade and contestable online markets, and ensures the internet is safe and secure, built on trust. The Declaration rightly recognises that, with the right conditions and principles, "the internet can deliver on the promise of connecting humankind and helping societies and democracies to thrive."

We would like to underline the importance of the **involvement of the full multistakeholder community throughout the entire Global Digital Compact process**, beyond this initial consultation. While adopted among governments at the United Nations, the Global Digital Compact will be implemented by private sector, civil society, technical community and governments – as such, the full community must be involved in its drafting.

Section 2 – thematic input

Connect all people to the internet, including all schools

CORE PRINCIPLES

Connecting all people to the internet requires effective action on all three layers of the ICT ecosystem: accessible and trustworthy **infrastructure and devices**; appropriate **applications and services** built on the infrastructure; and **digital skills**.

This requires policymaking based on two basic principles:

1. Public policies and regulations should promote the value of the **entire communications and digital services ecosystem**
2. Policies should **promote competition**, being technology-neutral, and supportive of innovative business models

In 2021, the **UN Broadband Commission Working Group** established as a strategic recommendation to increase broadband deployment by "broadening the base" of stakeholders: increasing the number of stakeholders that will support projects to increase both broadband deployment and adoption – particularly where market forces up to now have proven to be insufficient.

The report highlights the new realities of the digital economy in the 21st Century – more companies are creating value over existing network infrastructure beyond those who have traditionally invested in, funded, or financed such networks or contribute to extending universal service. In addition, there are new players building and investing in new infrastructure, often in partnership with traditional players. The report also notes that broadening the base could **create innovative and sustainable business models for the provisioning and use of broadband service** that address the challenging problem of extending broadband connectivity to underserved and often challenging areas.

Furthermore, the **Declaration on the Future of the Internet** establishes a number of important principles in this regard:

- Inclusive and reliable access to the Internet should be available for individuals and businesses and efforts to close digital divides should be undertaken to ensure everyone can benefit from the digital transformation – and rely on the principles of protecting individuals' privacy, their personal data, the confidentiality of electronic communications and information on end-users' electronic devices, consistent with the protection of public safety and applicable domestic and international law
- Digital literacy, skills acquisition, and development should be supported so that individuals can overcome the digital divide, participate in the Internet safely, and realize the economic and social potential of the digital economy
- Cultural diversity and multilingual content should be fostered, as well as social and digital inclusion within society, resilience to disinformation and misinformation, and participation in democratic processes

KEY COMMITMENTS

It is essential that all the actors of the internet ecosystem, with the support of governments and regulators, ensure the right competitive and regulatory environment maintaining trust in electronic communication services, contribute to support the deployment of next generation connectivity and reduce the digital divide. Industry leaders, stakeholders and policymakers need to engage in dialogue where this is not the case, to ensure that regulatory asymmetry, market distortions or other factors do not limit this ability, and that the right incentives for digital infrastructure investment are in place to support the long-term growth of the ecosystem.

Different approaches may be appropriate in different markets to address any market imbalances, however, the ultimate goal is nevertheless the same: to deliver and sustain digital connectivity — for everyone — for decades to come.

This includes:

1. Building a common vision and goals to provide the digital infrastructure that will connect all people to the Internet. However, this demands policies that promote a balanced digital ecosystem to ensure the sustainability of network investments.
2. Facilitating **investment** and promoting **innovative financing models** for the deployment broadband services and connectivity across the entire digital value chain. To promote remote and **rural connectivity** – specifically schools – policies should aim at reducing cost of deploying broadband access.
3. Ensuring that the allocation and licensing of **spectrum** should be transparent, fair, economically efficient, technology-neutral, and aimed at ensuring the availability of sufficient broadband-capable spectrum.

A number of ETNO members have signed up to the initiative of the International Telecommunication Union (ITU) Partner2Connect, which is a multistakeholder alliance with the objective of fostering **meaningful connectivity and digital transformation globally**. Such an initiative can provide an important framework for commitments of private sector, civil society and public bodies. In this context, some members commitments include, inter alia:

- Commitment to invest for connectivity, to increase voice and data coverage
- Education and training for a safe and responsible use of digital technology (including parents' use for child protection), and training to develop skills required to use digital tools
- Development of the appropriate regulatory and taxation environments to foster connectivity, digital literacy and inclusion

In addition, a number of ETNO members have made specific commitments to reduce the digital divide and improve digital equality, such as ensuring connectivity for all, providing inclusive offers and affordable devices, and helping people improve their digital skills. An example of this is the Orange commitment to digital equality. Similarly, Telefónica published a Rural Manifesto, a proposal for developing inclusive and sustainable rural networks, bringing together public and private efforts under a collaborative approach, and focusing on a new model that revolves around three main axes: innovation, cooperation and sustainability.

With respect to the **exploration of new investment models**, and in line with the recommendations of the **UN Broadband Commission's report**, governments should develop mechanisms to create the appropriate incentives and reforms to enable contributors to make even more investments.
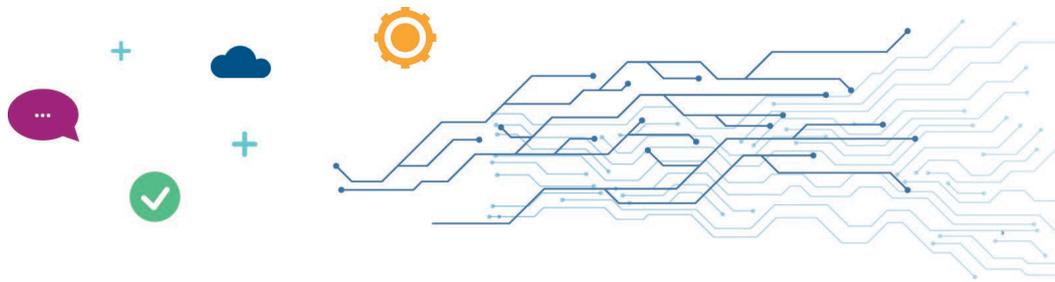
CORE PRINCIPLES

The functioning of an open, interconnected and interoperable internet can be undermined due to unintended consequences of technical, legislative, regulatory and policy developments that have an impact on the different layers of the Internet. Such threats include government-mandated internet shutdowns, the proliferation of cybercrime and low cybersecurity standards, and policies aimed at controlling access to the internet or conducting surveillance on the general public. Consideration should also be given to the possible technical fragmentation of the internet, which puts into question the interoperability and interconnectedness of the global internet.

As guiding principles, each actor in the multistakeholder community should commit to preventing **internet shutdowns**, ensuring common technological standards for the Internet architecture, the global **free-flow of information**, developing and promoting **high standards of cybersecurity** and confidence on the internet, and preserving the **multistakeholder** model of internet governance.

KEY COMMITMENTS

ETNO members take the commitment to the open internet seriously, in the understanding that a fragmented internet and low cybersecurity standards leads to a lower level of trust in the internet and digital technologies – for individuals, businesses, governments and society at large.

Our members support the Internet Governance Forum Policy Network on Internet Fragmentation (IPNF). This multistakeholder coalition aims to offer a systematic and comprehensive framework to define Internet fragmentation, its intended and unintended causes, and its potential effects; to collect and analyze case studies to fine-tune and complement this framework and to establish shared principles, recommendations or codes of conduct that prevent fragmentation and preserve the open, interconnected and interoperable nature of the Internet.

Internet shutdowns, including government-mandated shutdowns, are detrimental to trust in the internet and digital economy, to human rights, and to the economic prospects of individuals, businesses, countries and regions. Our members are strongly opposed to such measures, and any restrictions to internet access must be firmly grounded in international law, and have a legitimate legal basis.

With regard to **cybersecurity**, our members invest major resources in cybersecurity research and resilience measures to contribute to a robust cybersecurity environment, to protect the integrity and security of our networks themselves, and the data carried on those networks. Our members are engaged in a number of initiatives such as the International Communications CISO Council (ICCC), which brings together telecoms associations and major national ISPs, to exchange ideas and information, and contribute to enhancing cybersecurity globally.

CORE PRINCIPLES

The international transfer of data is an inherent part of the functioning of the world economy and social exchanges. In fact, organizations from all sectors, whether public or private, multinationals and SMEs, rely heavily on the possibility of transferring personal data in order to provide their services. Today, virtually no organization, regardless of sector, could engage in international trade without the ability to transfer data across borders. Data flows play an invisible but structural role in delivering products and services to citizens in their daily lives. The Global Digital Compact should recognise that establishing and maintaining trust, and minimising disruptions in data flows are fundamental to reaping the benefits of digitalisation. The Compact should call for the **removal of unjustified obstacles to cross-border data flows**, and encourage global cooperation and interoperability across policy and regulatory systems on data governance matters.

Citizens and companies need sustainable solutions in light of today's globalized economy and society, where international transfers of data are not an exception, but the general rule. A fundamental cornerstone of trust in the internet and digital technologies is the assurance that personal and other data is protected, both by a robust cybersecurity infrastructure, and a trustworthy legal framework for data protection. To ensure a trustworthy digital ecosystem, and guarantee that business can operate based on a clear legal framework across borders, governments and legislators should ensure that the policy and regulatory environments for data protection and data access are up-to-date and reflect the best practices in respect of privacy and security. The lack of interoperability across jurisdictions can create needless administrative burdens and compliance inconsistencies, which limits the potential of the global digital economy.

KEY COMMITMENTS

ETNO members maintain the highest standards of data protection, as enshrined in European legislation, in particular the General Data Protection Regulation (GDPR) and ePrivacy Directive. We are committed to the protection of personal data, including when it is transferred across borders. It is incumbent upon companies to implement their legal obligations to protect privacy and security of data, across the entire processing lifecycle or locations of processing.

The European Union has established a robust framework of data protection and access to data, with the twin aim of ensuring that the data of individuals, businesses and governments are protected; but also to give the possibility of using data to harness the potential of technology in driving the green transition, and develop citizen-centric public services: the right balance should be struck between the **ability to innovate, the protection of trade secrets and investments into the data economy,** and the **protection of individuals' personal data**, through the application of data protection by design, data protection impact assessments, and technical safeguards such as pseudonymization and encryption.

In this context, it is important to highlight that OECD countries recently adopted the first intergovernmental agreement on common approaches to safeguarding privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes. The **OECD Declaration on Government Access to Personal Data Held by Private Sector Entities** seeks to improve trust in cross-border data flows – which are central to the digital transformation of the global economy – by clarifying how national security and law enforcement agencies can access personal data under existing legal frameworks. It marks a major political commitment by the 38 OECD countries and the European Union that signed up to it during the OECD's 2022 Digital Economy Ministerial Meeting. The Declaration is also open for membership by other countries. This could be shared and proposed as a common framework on data flows and data privacy.
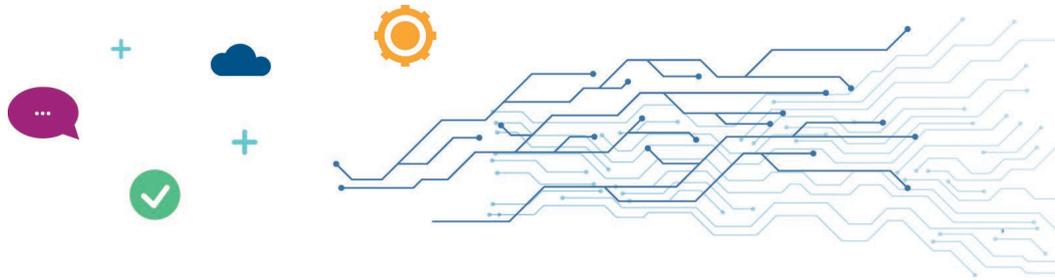
CORE PRINCIPLES

Rights that people have offline must also be protected online, in accordance with the rule of law and international human rights legal obligations.

With respect to the right to freedom of expression and privacy, these should be appropriately balanced with regulation on dealing with illegal content online, from copyright infringements, to the most heinous content, such as terrorist content and child sexual abuse material. European Union law is based on the principle of a **prohibition on the general monitoring of the internet**, which ensures that measures employed to tackle illegal content are targeted and proportionate to achieving that aim, while not compromising the rights of citizens.

KEY COMMITMENTS

Decisions on Internet governance and policy issues on all levels should be consistent with international human rights. The Global Digital Compact should reiterate governments' shared commitment to human rights and fundamental freedoms and recognize that rights people have offline must be equally protected online.
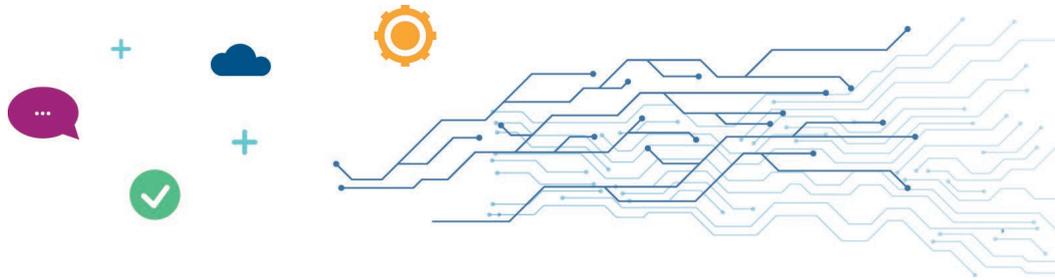
CORE PRINCIPLES

Artificial intelligence (AI) has enormous potential to transform our society and economy, harnessing the value of data to achieve efficiency gains and smart solutions, which will support in the twin green and digital transition. Governments and companies should promote innovative and trustworthy AI, which respects human rights and democratic values.

These value-based principles refer to:

- Stakeholders should proactively engage in **responsible stewardship of trustworthy AI** in pursuit of beneficial outcomes for people and the planet, such as augmenting human capabilities and enhancing creativity, advancing inclusion of underrepresented populations, reducing economic, social, gender and other inequalities, and protecting natural environments, thus invigorating inclusive growth, sustainable development and well-being.
- Developers and deployers of AI should respect the **rule of law**, **human rights** and **democratic values**, such as freedom of expression, dignity and autonomy, privacy and data protection, non-discrimination and equality, diversity, fairness, social justice, and internationally recognised labour rights.
- Developers and deployers of AI should commit to **transparency and responsible disclosure** regarding AI systems.
- AI systems should meet agreed standards of **robustness**, **security** and **safety**, and should meet these standards when deployed, and throughout their entire lifecycle.
- Developers and deployers of AI should be **accountable** for the proper functioning of AI systems.

KEY COMMITMENTS

ETNO is actively engaged in the Council of Europe's work in drafting a framework convention on Artificial Intelligence, which will set binding rules on risk assessment and mitigation for AI in three key areas: human rights, democracy and the rule of law.

In addition, our members support the other legislative and non-legislative initiatives. The OECD principles, which have been endorsed by G20, are an important cornerstone for the approach to trustworthy AI, and should form the basis of international initiatives on AI. The ongoing legislative work on an AI Act in the EU, underpinned by the European Commission's AI Ethics Guidelines, will create a worldwide precedent. Developed on a risk based approach, it must ensure an appropriate balance between innovation and regulation.
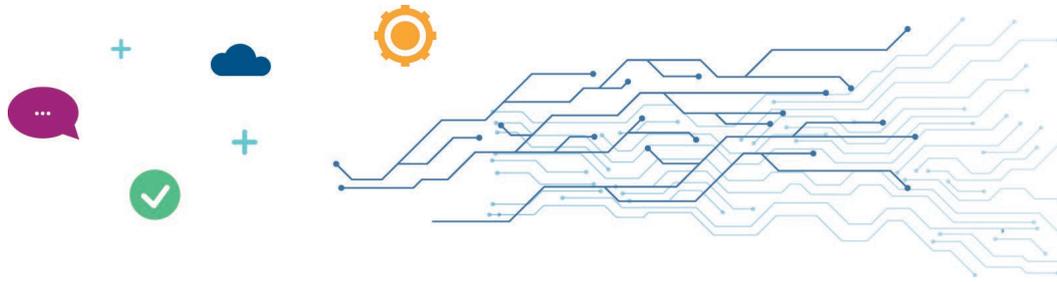
ETNO (European Telecommunications Network Operators' Association) represents Europe's telecommunications network operators and is the principal policy group for European electronic communications network operators. ETNO's primary purpose is to promote a positive policy environment allowing the EU telecommunications sector to deliver best quality services to consumers and businesses.

For questions related to this contribution, please contact:

Ross CREELMAN
Public Policy Manager, ETNO
creelman@etno.eu