



JOINT SUBMISSION TO THE GLOBAL DIGITAL COMPACT CONSULTATIVE PROCESS

GDC Principles & Commitments

The International Center for Not-for-Profit Law (ICNL) and the European Center for Not-for-Profit Law (ECNL) are pleased to prepare this joint submission to contribute to the consultative process for the Global Digital Compact led by the U.N. Envoy for Technology and co-facilitated by Sweden and Rwanda. We appreciate this opportunity to set forth the principles and commitments that we believe are vital for an open, free, and secure digital future for all. We look forward to engaging with this process before, during, and following the Summit for the Future in 2024.

CORE PRINCIPLES

Access to the global internet and the exercise of their rights. The promises of government digitization efforts, online public participation, and expanding civic space are a positive obligation to increase access and affordability for all

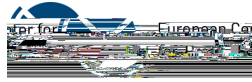
all people to the internet is a prerequisite to the development and adoption of technologies for public services.

Government actions that hinder access, connectivity, and affordability including through the imposition of onerous taxes, internet disruptions, SMS censorship, and website and application blockages undermine the goal of utilizing the internet as a means of exercising fundamental rights. Orders to restrict access to the internet must be provided by law, necessary to advance a legitimate aim, and narrowly tailored to achieve that aim. Full or partial internet shutdowns are never proportionate. Internet access and sharing critical information.

KEY COMMITMENTS

Through the Global Digital Compact, States should recognize that meaningful access to the internet is a human right and a key means to access other fundamental economic, social, political, and civil rights. To this end, States should commit to adopting laws and policies that facilitate internet access and promote internet affordability. Such laws could establish tax incentives for third parties to provide more affordable internet services. States should invest in connectivity and institute programs like universal service funds that cover the costs of internet access for marginalized groups. States should also implement digital literacy programs to increase the capacity of all people to engage online meaningfully and safely. States should repeal existing laws and desist from introducing new laws that impose taxes on use of the internet or impose other onerous barriers to internet access. They should also commit not to pass laws or issue extralegal orders that disproportionately disrupt or throttle the internet, in whole or in part. Meanwhile, international financial institutions that are enabling States to invest in infrastructure development should ensure their loan instruments reflect rights-based obligations to reflect the commitments above.

CORE PRINCIPLES





ÁfþÉ` ÖfC •›Ök›• ›] 1õþ„•CÁ 3„C ; Ö Éþ3}C4Ö° Éf›þ„; 3C ÁC4›^• communities and individuals, and legal restrictions should be put in place restricting surveillance-based business models.

Finally, there should be no exemptions from the highest standards of data protection for public institutions, including law enforcement, national security authorities, and counterterrorism agencies.

KEY COMMITMENTS

States should adopt and promote strong personal data protection rules and create well-resourced, independent offices responsible for enforcement. States should actively protect encryption and anonymity, including by adopting laws, regulations and policies that confer only on courts the power to remove the right to anonymity, only when necessary and proportionate, rather than on law enforcement agencies. States should also commit to pushing back against national laws enacted by autocratic leaders for surveillance and censorship purposes which require telecommunication companies

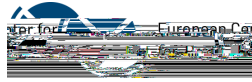
•; ›•„k•C ÉCÁõk4CÉ Ö› ÉÖ›ÁC 4kÖk C•É¼ ¼CÁÉ›• „ ; Ö k• ÖfC 4›

To ensure low-resourced organisations, including civil society organisations, are well-placed to conform to data protection rules, States should commit resources and time to providing technical assistance and tools that better enable compliance prior to rules coming into effect.

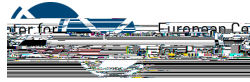
Relevant UN human rights treaty bodies and special procedures mandate holders should enhance their synergies and cooperation, including through joint action, to strengthen data protection standards of relevant rights holders (e.g., Human Rights Committee, UNSR on Privacy and Data Protection and UNSR on Human Rights Defenders, UNSR on Counter-Terrorism and Human Rights, UN on the human rights of migrants, Committee on the Elimination of Racial Discrimination, etc.).

CORE PRINCIPLES

The core principle that the same rights that apply offline also apply online should guide all components of the Global Digital Compact, and not be relegated to its own issue area. Furthermore, human rights protections should be the cornerstone of all online activities, either by public bodies or private entities



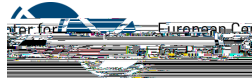
or metadata like location or IP address) must be based on a relevant law, necessary and



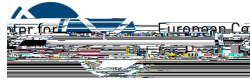
controls or possibilities to sanction governments, companies, organisations, and individuals that do not abide by these principles.

The UN Tech Envoy should ensure a multistakeholder approach is implemented throughout the UN digital work and that civil society stakeholders are informed about the modalities of the negotiation and drafting process.

Large tech companies need to commit to maintaining safe spaces, making their tools available in recognized languages, upholding individual and collective rights, and addressing accessibility concerns. They should conduct human rights due diligence on their services, products and activities, including content policies, and ensure meaningful participation of civil society and affected communities. Effective internal grievance mechanisms should be established to appeal content decisions and other decisions affecting users. States should enact laws that grant users whose content wa-2(bm)8)JTETQ0.000009



ICNL



International Non-Governmental Organisations (CINGO) of the Council of 1 P Á › ¼ C ¾ É
Committee on Artificial Intelligence.

INTERNATIONAL CENTER FOR NOT-FOR-PROFIT LAW