Donor Principles for Human Rights in the Digital Age

Developed through consensus by the Freedom Online Coalition's 38 Member States, with input from the independent multistakeholder FOC Advisory Network, and other stakeholders.

View the Donor Principles online:
www.freedomonlinecoalition.com/donor-principles-for-human-rights-in-the-digital-age/

FREEDOM
ONLINE
COALITION

Donor Principles for Human Rights in the Digital Age

Freedom Online Coalition – October 2023

Preamble

The Donor Principles for Human Rights in the Digital Age call on governments with international development and assistance programming to advance an affirmative, rights-respecting agenda for our collective digital future that upholds our commitment to 'do no harm.' They are driven by the ideal that donors should invest in digital technologies and data collection only when it is possible to protect against their potential misuse, and when procedures are put in place to facilitate this protection. The Principles align with the broader vision that, to enable individual dignity and economic prosperity, technology should be harnessed in a manner that is open, sustainable, secure, and respectful of democratic values and human rights.

In recent years, donors have increasingly invested in digital initiatives across international assistance and development sectors, frequently with positive outcomes. As technological innovation has accelerated, however, it has outpaced donors' ability to constrain potential harms. In the absence of robust safeguarding, the same digital technologies that have brought benefits to populations around the world have also contributed to the erosion of human rights protections and democratic institutions, processes, and norms. These negative effects have been acutely felt by those in the global majority,[1] and especially persons in vulnerable situations who have limited influence over how decisions are made about technologies' development, deployment, governance, and use.

The Principles aim to increase donor accountability in this rapidly changing digital age by providing a normative blueprint for how donor governments should align their investments and engagements with their commitments to human rights and democratic values.[2] The Principles serve as a resource for donor agencies as they develop strategic priorities and institutionalize processes and structures that shape foreign assistance. Given the Principles' strong focus on donor commitments to human rights and democracy, they have been drafted and negotiated through the Freedom Online Coalition, a multilateral coalition of member governments—and a multistakeholder advisory network—committed to protecting human rights online and in digital contexts.

The Principles are grounded in international human rights frameworks, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the UN Guiding Principles on Business and Human Rights. The rights that are particularly relevant to these Principles include freedoms of expression, association, and peaceful assembly; privacy, non-discrimination; and the ability to seek, receive and impart information; among others.

[1] Also known as 'global South.'

[2] The Donor Principles for Human Rights in the Digital Age complement an existing set of Principles for Digital Development. Please see Principle #9 for more information.

Donor Principles for Human Rights in the Digital Age

1. Support partner countries to align their legal and regulatory frameworks and technical standards with international human rights considerations.

2. Support the development and implementation of digital government and data management systems that promote and strengthen democratic governance and respect for human rights.

3. Collaborate with the private sector to drive rights-respecting investment and innovation and advance shared goals.

4. Request an impact assessment process for how human rights considerations are integrated into all programs with digital components.

5. Prioritize digital inclusion, including by engaging with stakeholders, supporting local research, and leveraging resources from local digital ecosystems.

6. Foster coordination and strengthen alliances between stakeholders and among donor governments.

7. Support the growth of a rights-respecting technology workforce.

8. Prioritize digital security and safety in the development and implementation of programs, the use of digital tools, and the management of data.

9. Adopt and promote the Principles for Digital Development, including by integrating digital solutions across sectors and programs, if appropriate.

1. Support partner countries to align their legal and regulatory frameworks and technical standards with international human rights considerations.

Donors should synergize their support for digitalization with support to prevent or mitigate its misuse as part of a comprehensive, strategic approach to digital transformation. For example, international assistance for the digitization of government systems, expansion of digital services, or digital innovation should be accompanied by support for countries to align their domestic legal and regulatory frameworks on issues such as data protection, access to information, cybersecurity, online safety, and anti-defamation with their international commitments to human rights and democracy.

Donor governments should encourage and facilitate multistakeholder processes for drafting legislation—including government, industry, civil society, and academia—and support the implementation and oversight of relevant laws and frameworks. Similarly, donors should foster the meaningful and sustainable participation of civil society advocates and human rights experts in technical standard-setting bodies and processes,[3] where the parameters for the design of new and emerging digital technologies are set.

Potential topics that donor support might address include technology-facilitated gender-based violence; unlawful or arbitrary digital surveillance that leads to restrictions on freedoms of expression, association, or peaceful assembly; the exploitation of personal data without consent; and the use of biased data in artificial intelligence (AI) machine learning models. Adverse impacts can emerge from the intentional exploitation of digital data—e.g., a government unlawfully collecting journalists' digital data in order to threaten them—or unintentional exploitation—e.g., a government using a dataset not representative of the population to allocate public services.

[3] Relevant technical standards setting bodies include the World Wide Web Consortium (W3C), the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), the International Telecommunications Union Telecommunication Standardization Sector (ITU-T), the International Organization for Standardization (ISO) and the Internet Corporation for Assigned Names and Numbers (ICANN), as well as national standard-setting bodies.

2. Support the development and implementation of digital government and data management systems that promote and strengthen democratic governance and respect for human rights.

Digital government and data management systems include digital platforms that facilitate internal government operations and external service delivery—e.g., for healthcare, social services, education, taxation, policing, court systems, or electoral processes; physical data centers and onsite and cloud-based databases that organize, store, and manage citizen data and other information; and data exchange platforms that facilitate the movement of data from one platform or database to another. Increasingly, such systems are integrating AI, which can automate aspects of government decision-making. Components of these systems that are built using open source technology are oftentimes referred to as digital public infrastructure or digital public goods.[4]

When procured, managed, and governed in alignment with respect for human rights, these systems can enhance government transparency and accountability, foster citizen participation in the political process, enable inclusive access to government services, and generally strengthen the relationship between the government and the governed, while also protecting personal privacy and security. Donors should support a human rights-based approach to cybersecurity and personal data protection in the development, management, and governance of these systems to help safeguard them against purposeful and inadvertent misuse and abuse. This includes prioritizing and strengthening monitoring and accountability processes at the national and international level. Donors should also support processes for public service software and infrastructural development, and should strive to support open source technology when appropriate. Given the strong human rights implications of climate change,[5] and the massive energy outputs required to establish and maintain digital and data management systems, donors should also emphasize energy efficiency in digital transformation.

[4] For example, the Digital Public Goods Alliance, which defines digital public goods as open-source software, open data, open AI systems, and open content collections that adhere to privacy and other applicable best practices, do no harm by design and are of high relevance for attainment of the United Nations 2030 Sustainable Development Goals (SDGs).

[5] See, for example, the United Nations Office of the High Commissioner for Human Rights report, Understanding Human Rights and Climate Change.

3. Collaborate with the private sector to drive rights-respecting investment and innovation and advance shared goals.

The private sector, including investors, companies, and company shareholders, plays a critical role in shaping countries' digital ecosystems. Donor governments should take concrete steps to foster private sector collaborations and commitments that are grounded in respect for human rights. This includes facilitating investments in infrastructure, education, and training, particularly for small- and medium- sized enterprises (SMEs), and partnering through programmatic and non-programmatic means to uphold shared commitments to respect human rights and enhance individuals' and groups' safety and security. Donor governments should also emphasize the need for industry to remain accountable to address critical feedback from civil society and human rights defenders.

Transnational private sector companies often have weak direct connections to local civil society stakeholders and other civic actors, especially in global majority countries. When appropriate, donors can help strengthen those connections by leveraging their convening power to create opportunities for private sector partners to work with and learn from civil society and academia. Donors can and should hold private sector partners accountable for making inclusive, sustainable, and rights-respecting business investments, including in the design, testing, and deployment of their technologies. Donors should also hold privacy sector partners accountable for fulfilling their commitment to respect human rights in alignment with the UN Guiding Principles on Business and Human Rights.

4. Request an impact assessment process for how human rights considerations are integrated into all programs with digital components.

In alignment with a 'do no harm' approach to digital development, donors should undertake a periodic due diligence process to identify human rights implications of all programs with digital components across development sectors and throughout the entire technology stack. In the context of multi-donor or multilateral engagements, donors should also encourage other stakeholders involved to do so. Donors should establish clear thresholds for when to undertake a full Human Rights Impact Assessment (HRIA)—as outlined in the UN Guiding Principles on Business and Human Rights[6]—in order to identify, prevent, mitigate, and account for the potential and actual human rights impacts of international assistance programs with digital components.

An HRIA is an iterative process that is developed and administered transparently: it includes meaningfully consulting with potentially affected stakeholders and civil society to identify the risks to human rights prior to implementing a program, and monitoring risks and human rights impacts over the program's lifecycle. HRIAs can inform donor decisions about how to build, fund, and integrate new digital platforms and tools across sectors. They can also be used to convene interested parties and publicly justify donor decisions.

Other types of impact assessments—e.g., Algorithmic Impact Assessments (AIA) or Data Protection Impact Assessment (DPIAs)—can be implemented as a component of, or in some cases instead of, a full HRIA. DPIAs and AIAs can be used to identify and mitigate potential risks and impacts arising from the development and deployment of an algorithmic system (in the case of an AIA), or technologies that track, monitor, or process peoples' personal data (in the case of a DPIA). The impacts considered in AIAs and DPIAs concern individual human rights, as well as, for example, health, safety, and physical security. As part of general due diligence processes, donors can also support stakeholders that receive international assistance to conduct impact assessments of their own digital systems and policies.

[6] See especially pp. 17-24.

5. Prioritize digital inclusion, including by engaging with stakeholders, supporting local research, and leveraging resources from local digital ecosystems.

Digital inclusion refers to the meaningful contribution by diverse stakeholders to the design, development, deployment, use, governance, and assessment of digital technologies. By default, digital systems prioritize the needs of the people who pay for and create them, and reflect their values and assumptions about the world. Individuals and groups in vulnerable situations are also disproportionately negatively impacted by the misuse of digital systems. By prioritizing inclusion, especially civil society actors, small- and medium-sized enterprises (SMEs), and individuals and groups who experience vulnerability, marginalization, or exclusion, donors can foster more representative and thus more democratic and safer digital ecosystems. In particular, donors should consider women and girls in all their diversity, and LGBTI persons.

Donors can facilitate inclusion by supporting educational models that equip diverse stakeholders with the knowledge, skills, and tools necessary for meaningful participation in digital decision-making; promoting the growth of local technology sectors; supporting locally developed digital content and services; and facilitating civil society actors' and technologists' representation at regional and international forums focused on data and internet governance. Donors should also consider that those who may not use digital technologies in their everyday lives are nevertheless impacted by decisions made about technologies' development, use and governance. Internally, donors should develop inclusive, consent-based processes for collecting data on affected populations, and support the use of equitable data for program development and assessment.

6. Foster coordination and strengthen alliances between stakeholders and among donor governments.

Multistakeholder engagement, which includes government, industry, civil society,[7] media, and academia, drove the Internet's democratic development at its inception, and remains the best way to foster democratic decision-making about digital technologies' role in society. Facilitating collaboration between civil society and technology experts in local geographies, in particular, can help increase the likelihood that the development and design of digital technologies in specific contexts is aligned with the needs and desires of local populations, and does not cause undue risk or harm.

Donor governments have the opportunity to help shape common visions, standards, and goals around their investments in digital contexts, and to inform ongoing processes to develop and implement global governance frameworks for digital technologies. Through regular strategic multistakeholder engagement, and coordination and collaboration both within governments and between them, donors can fulfill their commitment to protect human rights by aligning efforts to support countries' digital transformations with efforts to protect against potential misuse and abuse, enhancing the overall efficiency and effectiveness of their foreign assistance. To this end, donors should actively coordinate to identify and share practical approaches that they can use to concretize these Principles for Human Rights in the Digital Age into their processes and programs.

[7] Please see the OECD DAC Recommendation on Enabling Civil Society in Development Co-operation and Humanitarian Assistance https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-5021

7. Support the growth of a rights-respecting technology workforce.

Software engineers, data scientists, User Experience/User Interface (UX/UI) designers, product managers, and trust and safety staff collectively shape the technology products that structure our world, and executive level decision-makers set the priorities that inform the design and development process. When engaging companies, academia, and others, donors should encourage these products to be built in alignment with respect for human rights and democratic values by supporting inclusive "human rights by design" processes,[8] and the hiring and promotion of talent with multidisciplinary experience across the humanities and sciences. This is especially critical for emerging technologies.

Donors should also support education efforts that foster greater understanding and application of human rights considerations in technical design and development. This could include support for the enactment and application of a professional code of ethics for individuals, organizations, and institutions involved in the technology development lifecycle as one way to encourage that they be trained on and act in accordance with ethics and respect for international human rights.

[8] Human rights by design processes should include consultations with local civil society actors, human rights defenders, and other affected stakeholders.

8. Prioritize digital security and safety in the development and implementation of programs, the use of digital tools, and the management of data.

Donors should prioritize digital security and safety for staff, implementers, and beneficiaries, with a particular focus on the protection of privacy of individuals and groups who experience vulnerability, marginalization, or exclusion. Digital security and safety should be integrated into internal processes and the lifecycle of programs, including during project or activity design, development, implementation, and closeout. Donors should ensure that they and their implementing partners have access to the resources and expertise required to do so. Such considerations should be incorporated into solicitations and budgeted for accordingly. In addition to allocating program funds towards these efforts, donors should explore mechanisms for flexibly supporting their implementing partners in ongoing risk assessment, incident/emergency response, and program adaptation in response to unexpected changes in their threat landscape.

9. Adopt and promote the Principles for Digital Development, including by integrating digital solutions across sectors and programs, if appropriate.

The Principles for Digital Development, initially drafted in 2012, provide guidance to help donors and implementing partners integrate good practices into digital technology-enabled development and humanitarian assistance programs, with the goal of overcoming the major barriers that these initiatives face. The Principles for Digital Development have been endorsed by more than 300 organizations and are stewarded by the Digital Impact Alliance (DIAL).

Collectively, the Principles for Digital Development and the Donor Principles for Human Rights in the Digital Age offer a comprehensive blueprint for responsible, rights-respecting, and effective investments and engagements across international development and assistance in digital contexts. While the Donor Principles for Human Rights in the Digital Age guide provide a normative framework to guide donor agencies as they develop strategic priorities and institutionalize processes that shape foreign assistance, the Principles for Digital Development guide program implementers - in donor governments and implementing partner organizations – as they design and implement programs, projects, and activities. The Donor Principles for Human Rights in the Digital Age, which focus on the implications of digital technologies for human rights and democracy, articulate the normative basis for rights-respecting digital development in the 21st century, while the Principles for Digital Development, which focus on maximizing the effectiveness of digital development programs, provide implementers with a toolkit for doing so.

When adopted and promoted together, the two sets of principles can help facilitate digital development that is responsible, sustainable, inclusive and rights-respecting, and inform donor decisions about whether, and to what extent, digital components should be developed and integrated into programs.