



**2020**

**Recognizing Human Rights Norms in the  
“Principles on Identification for  
Sustainable Development”:  
Civil Society Consultation Report**

## CONTENT

1.0 Introduction	2
2.0 General Feedback – Themes and Overarching Input for Improving the Principles Document	3
3.0 Specific CSO Terminology Recommendations for the Principles Document	6
4.0 Role of IOs and IO-CSO Engagement	7
5.0 Conclusion – Ongoing Collaboration	10
ANNEX	11

---

## ACRONYMS AND ABBREVIATIONS

CSO	:	Civil Society Organization
EOs	:	Endorsing Organizations
ID4D	:	Identification for Development
IO	:	International Organization
SDGs	:	Sustainable Development Goals
UDHR	:	Universal Declaration of Human Rights





## 1.0 Introduction

The **Principles on Identification for Sustainable Development** (the Principles),<sup>1</sup> the creation of which was facilitated by the Identification for Development (ID4D) team at the World Bank in 2017, provide an important framework for the development of digital identification (ID) systems across the world. They are endorsed by many global and regional organizations (the “Endorsing Organizations”) that are active in funding, designing, developing, and deploying digital identification programs across the world, especially in developing and less developed countries.

As an international finance institution, the World Bank facilitated the process of creating the Principles from a development perspective and focus. Given that digital identification systems are being deployed in countries with varying levels of technological, economic, infrastructural, and governance-related development, it is important that stakeholders<sup>2</sup> — and the frameworks that guide their decision-making — pay cognizance to the needs and realities of the people living in regions and national contexts in which digital identification investments have skyrocketed.

During 2020, a consultation process focused on gathering input for the first review and revision of the Principles. Alongside that process, Access Now, Namati, and the Open Society Justice Initiative co-organized a Civil Society Organization (CSO) consultation on August 24, 2020 with the World Bank’s ID4D team, Endorsing Organizations (EOs) and over 60 Civil Society Organizations, to discuss the Principles, the role of the EOs and CSOs broadly in the digital identification space, and to devise mechanisms for greater institutionalized engagement between CSOs, the World Bank and EOs, and other international organizations.<sup>3</sup> The participating CSOs thanked the ID4D team for the opportunity to participate in the consultations and the recognition of the important role CSOs play in the development of inclusive and human rights-honoring digital identification systems, particularly at national and local levels.

This Report presents a summary of the top-level comments and discussions that took place in the meeting from the perspective of the CSO participants.<sup>4</sup>

1 World Bank (2018). Principles on Identification for Sustainable Development: Toward the Digital Age. <http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf>

2 For purposes of this Report, the “stakeholders” include the World Bank, the Endorsing Organizations, national governments, international institutions and agencies, CSOs and the public. This is not an exhaustive list.

3 A list of the participating CSOs is provided in Annex A at the end of this Report.

4 Note that this Report was developed by a working group of CSOs that participated in the consultation. The recommendations in this Report are intended to capture collectively the comments made during the meeting but do not necessarily reflect the views of each CSO in all respects.



## 2.0 General Feedback – Themes and Overarching Input for Improving the Principles Document

2.1 The Principles offer a brief and insufficient reference to human rights. Now that we are on the verge of an explosion in the integration of digital identification systems, there is an urgent need for human rights criteria to be recognized as a tool for evaluation and oversight.

As reflected in the Universal Declaration of Human Rights (UDHR),<sup>5</sup> the recognition and enforceability of human rights rests on three fundamental principles:

1. Human beings with autonomy and moral responsibility (human autonomy),<sup>6</sup>
2. Human beings with free will to act or not to act (human agency),<sup>7</sup> and
3. Human beings with subjective rights that are limited by responsibilities in relation to other individuals and the community (authority structures).<sup>8</sup>

In discussions about digital technologies overall, these principles are commonly applied as rights to privacy, expression, inclusion and non-discrimination, and freedom of conscience.

Digital identification systems raise important international human rights and broader legal considerations with respect to the way information and actions are linked to persons, authenticity is proven, and individual rights and responsibility is determined in systems. At the same time, this linkage between persons and networked machine systems enables the ability for systems to control human conscience and beliefs, behavior, and relations. Once deployed, digital identification systems can be powerful tools used for techno-social engineering, censorship, exclusion, discrimination, persecution, targeted deployment of social credit systems, torture, and surveillance – all intended to achieve and/or enhance obedience to authority structures.

Digital technologies by themselves do not necessarily threaten human rights. Instead, the threat comes from the purposes and values (i.e. 'the ends') embedded within the systems controlled by human-designed software code and algorithms, and the end uses to which they are put. The principles of the UDHR and other sources of human rights in international law can be applied effectively to limit the structures, purposes and uses of digital identification systems in the digital network-based environment. Of special concern for CSO participating in this consultation is the deployment of digital identification systems in pre-existing environments pervaded by structural discrimination, in support of social credit systems and techno-social engineering of human decision-making. Hence, the Principles need to incorporate and sufficiently reference human rights and human rights criteria as a tool for evaluating existing and proposed digital identification projects.

<sup>5</sup> The UDHR is available at <https://www.un.org/en/universal-declaration-human-rights/>. The authors note that the principles of the UDHR have been incorporated in a wide variety of United Nations documents, including the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social, and Cultural Rights.

<sup>6</sup> See Article 1 of the UDHR ("All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.")

<sup>7</sup> See Article 6 of the UDHR ("Everyone has the right to recognition everywhere as a person before the law.")

<sup>8</sup> See Article 29 of the UDHR ("(1) Everyone has duties to the community in which alone the free and full development of his personality is possible. (2) In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society. (3) These rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations.")

## 2.2 CSOs need to be formally recognized as partners with governments and corporations in designing and implementing digital identification systems.

CSOs have emerged as leading advocates for assessing the human rights implications of the growing corporate and governmental surveillance of the lives of ordinary people. Attention has been most notably brought to the risks posed by digital identification systems to individual privacy, access to private and public services, rights to expression, and freedom of conscience. Less attention is paid to the exclusionary impacts of systems, and a failure to identify and mitigate the known risk that digital identification systems pose will exacerbate discriminatory structures on the basis of protected categories, including race, religion, political opinion, caste, ability, age and gender. To best address these risks and ensure the application of human rights criteria to digital ID system design, implementation, and oversight in various national deployments, systematic, institutionalized CSO participation must be required by the World Bank. The consultation is a promising, necessary, first step, but it must be only the beginning.

## 2.3 The Principles must be meaningfully and transparently applied to digital identification system design and implementation.

The Principles are designed to guide the implementation of digital identification systems in practice, which includes aspects of the conception, development, technical design and operation of such systems that are still opaque to the general public and CSOs alike. During the consultations, participants stressed the need for heightened transparency in all phases of a project, including diagnostics, design and procurement of system components, with a meaningful opportunity to inform, and where necessary, to challenge these critical decisions and ensure broad public understanding and participation throughout. During the consultation, civil society actors from a range of national contexts also stressed the difficulties they faced in their work in simply understanding the basic aims, project design, key actors and implementation timeframe for digital identification programs. It is all the more imperative, then, that tools like data protection and human rights impact assessments are the rule, rather than the exception, in the process of design and public consultation regarding the introduction of new identification systems.





## 2.4 Ensure explicit commitment to the Principles along with commitment to not be involved in projects which do not abide by the Principles

It is of utmost importance that the Principles truly respect the rights of individuals impacted by digital identification programs, as the Principles guide the decision-making of the EOs. In many instances, CSOs have observed that signatories to the Principles have been involved in digital identification projects that do not respect human rights — or the Principles themselves. The participants during the consultation urged that the signatories affirm and commit to these Principles. Each signatory to the Principles must affirm that they will be involved only with programs that align with each tenet of these Principles and commit to restrict funding and support to programs that do not abide by the Principles. For the Principles to be effective, it is essential that such commitments be made, and for them to truly guide the behavior of the supporting organizations.

## 2.5 Digital identification system governance requires democratic processes and the rule of law

CSOs expressed the need to emphasize the importance of a transparent and democratic process in the development of identification systems. For example, we see systems pushed through by decree, or without a full and proper debate through the participatory channels that are part of a democratic process. This is to the detriment of the identification systems themselves because it loses legitimacy, and with the bypassing of a legislative process and public participation, perspective is lost on the safeguards that must be in place to guarantee human rights.

CSOs welcomed the proposed new section on, “**Why building ‘good’ digital ID is essential to mitigating risks,**” in the introduction to the Principles. However, CSOs felt these risks should be explained in more detail, to emphasize the range of risks and the weight of their potential impact. In addition, the risks outlined in the document should more closely link to the Principles themselves – ensuring the Principles address the key risks directly throughout the document, which would illustrate how the Principles are designed to mitigate the very risks identified in the introduction.



For example, to give a balanced account of the impact of digital identification systems, the reference to the SDGs in the introduction to the Principles should highlight how these systems place the achievement of the goals at risk. This can include how digital identification systems can lead to exclusion from government social security systems, which hampers achieving several targets in **Goal 1** on ending poverty, and **Goal 2** on ending hunger. **Goal 4** on education cannot be achieved while education is dependent on a child or their parents requiring specific identification documents. The target in **Goal 9.c**, on the access to information and communications technology and universal access to the Internet, is hampered by the exclusionary



need for SIM card registration. The effect of requiring digital ID as a prerequisite serves to exclude people from having decent housing (**Goal 11**) and rights in the workplace (**Goal 8**). Overall, the CSOs highlight the overall risks of exclusion resulting from layering digital identification on top of existing discriminatory legal frameworks or in countries that are not signatories to various conventions, such as Refugee and Statelessness Conventions.

### 3.0 Specific CSO Terminology Recommendations for the Principles Document

Many participating CSOs provided specific comments on the text of the Principles, during the virtual consultation and in individual and organizational written comments. These written comments are collected in an open-access compendium compiled by CSO participants.<sup>9</sup> The following provides a non-exhaustive list of specific language recommendations, which reflect the high-level input shared during the consultation meeting and summarized within this report.

**3.1 Principle 1** should clearly state a human rights focus. We could recommend that it be amended as follows: “Ensure human rights are respected for individuals and communities.”

**3.2 Principles 2 and 7** should be improved so that access to birth and death certificates and ‘legal identity’ credentials is given an equitable logic, that is, for people who cannot pay, they must be free as often as necessary.

**Principle 2** states that only the originally-issued birth and death certificates, along with the initial issue of a mandatory ‘legal identity’ credential, should be free of charge to the individual. This is limiting from a human rights perspective because it ignores the situation of people in a more vulnerable state. The elimination of barriers requires that everyone be equitable treated so that those who can afford some of the costs will pay the lowest price for the service and those who cannot, should still be granted access, duplicates included. Most of the economically vulnerable people are also vulnerable in many other aspects of life. They may reside in precarious housing, poorly resilient to weathering, or without any housing at all.

This means that they are often unable to keep their documents for life. In this sense, it is important to make explicit the guarantee of equity so that low-income people have access to the digital identification system in a more comprehensive way. Thus, free access for these people to duplicate documents that have been lost or damaged should also be an explicit recommendation. It is important to highlight that such a measure would not reflect on individuals overlooking the value of personal documents. It would remain the same, even with gratuity. This is because documentation by itself is valuable and the time spent on administrative procedures to obtain a new one will be already an incurred cost.

<sup>9</sup> Several CSOs made separate submissions to the ID4D team with specific feedback on the Principles. These submissions are available at: <https://drive.google.com/drive/u/0/folders/1zNbCekmCwpyDxWPajlz1LYEabGk77mM>

- 3.3 Principle 3's** heading should clearly reflect the need to embed human rights protecting designs: Instead of referencing the vague concept of a unique and accurate identity as a design focus, it should say "Protect human rights through system design". This would also provide a nice balance with Principle 6, which focuses on privacy-enhancing design.
- 3.4 Principle 8** should be amended to clearly reflect human rights principles – "Safeguard human rights, personal data protections, and privacy through a comprehensive legal and regulatory framework." And the second paragraph should be changed from "user rights" to "human rights" so as to give it a less technical emphasis. Finally, the reference to "undue" in discussing corporate surveillance should be omitted because of the human rights risks of purposing digital identification to facilitate commercial surveillance in any manner.
- 3.5 Principle 10** should expressly mention CSOs as being part of the digital identification system design and oversight committees/bodies.
- 3.6 A new principle** is needed to address facial recognition and other biometric authentication methods that allow the profiling of individuals without consent and are known to disproportionately discriminate on the basis of color and gender.

## 4.0 Role of IOs and IO-CSO Engagement

### 4.1 Digital identification system design, evaluation, and oversight

In order to facilitate streamlined and inclusive feedback and engagement with EOs, the CSOs suggested that each EO must be open to feedback on their projects to ensure they are in consonance with the Principles, and if any project is found wanting in this regard, the EOs must commit to rescinding their participation.

To ensure a constructive feedback loop, the CSOs suggested that each EO institute formalized CSO participation mechanisms to

1. Evaluate and analyze human rights impact of digital identification systems,
2. Advise the EO on its policies on digital identification, and
3. Act as a platform for CSO feedback and reporting on on-ground impact of digital identification systems.

But for CSOs to serve this function, funders of digital identification systems will need to find mechanisms – ideally ones with independent decision making - to extend financial resources to CSOs.

## 4.2 Need for greater country-level engagement at the earliest stages of potential projects

CSOs suggested building in a process or structure for CSO engagement within country-level projects from the earliest stages of a project. A primary challenge for civil society in many places is the complete lack of transparency around new digital identification systems. There is often little to no information made public about a proposed system until it is almost ready for roll-out, thus limiting the ability of both civil society and the public to provide input into the process, including highlighting risks, sharing information from ongoing community-level engagements, or providing alternative options within policy or system design decisions.

A structure for CSO engagement that starts from the earliest stage, such as a diagnostic before a project is even in motion, and that extends throughout the process would help cultivate greater trust in the digital identification initiative. Sustained CSO engagement would also ensure the system design (from the legal framework to operationalization) better meets the needs of people, including the most vulnerable. Again, the CSOs emphasized the need for financial resources to sustain such a level of engagement.

## 4.3 CSOs as co-anchors of the Principles

While acknowledging the critical work of ID4D to develop and steward the Principles, with a changing digital ID landscape and the importance of bridging the intersection between the development and the human rights needs of the Principles moving forward, as outlined in a number of submissions, CSOs raised the benefits of exploring a co-anchor model.<sup>10</sup>

ID4D, and the World Bank more generally, wear a variety of hats when it comes to digital identification systems: they provide expertise and analysis, often in a way that is not made public, and are a major source of funding. This variety of roles is not entirely compatible with ID4D's 'ownership' of the Principles which will guide digital identification systems in many countries. Given that so much of the work done by ID4D is, by necessity, not public, it becomes unclear as to how the Principles are implemented in practice. Similarly, it is the case that achieving the goals of ID4D means that it (the ID4D team) is perceived (whether accurately or not) as not being a 'neutral party' in these key debates, but rather as one of the most powerful and forceful proponents of these systems. However, Principles anchored in a more neutral approach by or in combination with CSOs would increase the power and influence of the Principles in governing activities in the digital identification space.

<sup>10</sup> For an example of a constructive co-anchor model between international organizations and CSOs that focuses on normative standards and national developments see the co-chair model of the Inter-Agency Working Group on Child Detention, available at: [https://endchilddetention.org/wp-content/uploads/2016/09/IAWG\\_Advocacy-Brochure\\_Aug-2016\\_FINAL-web.pdf](https://endchilddetention.org/wp-content/uploads/2016/09/IAWG_Advocacy-Brochure_Aug-2016_FINAL-web.pdf).





## 5.0 Conclusion – Ongoing Collaboration

Formal engagement of CSOs by the World Bank, EOs, and national governments is essential for ensuring that the Principles integrate human rights as required criteria for all considerations related to digital identification. CSOs have a broad understanding of the human rights implications as gained through lived experiences with identification systems, both paper-based and digitized.

Digital identification systems pervade the lives of individuals, become gateways for important services, and in most instances, become the foundation for a person's legitimacy or citizenship in a country or region. These digital identification systems and technologies have very real impacts on daily lives and societies. And the human rights-related risks most acutely affect marginalized and less privileged individuals.

The CSO participants thank the ID4D team for affording these consultations and look forward to continued discussions.<sup>11</sup> At the same time, the participating CSOs remain in dialogue with each other and stand behind the urgent need to embed human rights principles in the design and implementation of digital identification systems that the World Bank and other Endorsing Organizations are choosing to fund and support.

---

<sup>11</sup> The CSOs appreciate the offer by the ID4D team to share existing good digital identification system practices at the country level. The CSOs welcome receiving this information and engaging in further dialogue with the ID4D team from the perspectives of their own experiences about what may and may not work effectively for country-level engagement. CSOs note the need to focus on evidence-based good practice examples.



## ANNEX A

**Civil Society Consultation and Dialogue Meeting on the  
“Principles on Identification for Sustainable Development” and Digital ID**

**August 2020  
Participating Organizations**

<b>Organizations</b>	<b>Focus country/countries</b>
Access Now	Global
Africa Matters Initiative	Tunisia
AfroLeadership	Francophone Africa
ARTICLE 19 Eastern Africa	14 Eastern Africa countries
Asociación por los Derechos Civiles	Argentina/Latin America
BRAC, Human Rights and Legal Aid Services	Bangladesh
Braveheart Foundation	Myanmar
Canadian Civil Liberties Association	Canada
Charitable Fund Right to Protection	Ukraine
ChF “The Right to Protection”	Ukraine
CIS India	Global Focus
Civil Pole for Development & Human Rights	Tunisie
Collaboration on International ICT Policy for East and Southern Africa (CIPESA)	Global
Commonwealth Human Rights Initiative	India
Derechos Digitales	Latin America
Development and Justice Initiative	India
DHRRA Malaysia	Malaysia & Asia Pacific
Digital Welfare State & Human Rights Project, NYU Law School	Sub-Saharan Africa
Give1 Project Gambia	The Gambia
Haki na Sheria Initiative	Kenya
Homo Digitalis	Greece/EU
Human Rights Advocacy and Research Foundation (HRF)	India
IFRC	Global
Independent Expert	USA, Ethiopia, Kenya, Tanzania
Independent Expert	India
Initiatives for Dialogue and Empowerment through Alternative Legal Services	Philippines
Innovation For Change South Asia	South Asia
Institute of Advanced Studies, University College London	East Africa/Kenya and UK
Institute of Technology and Society - ITS Rio	Brasil
Jamaicans for Justice	Jamaica
KICTANet	Kenya



Lawyers Hub Kenya	Sub Saharan Africa
Makerere University	Uganda
Makerere University School of Public Health-Resilient Africa Network (RAN)	Across Africa
Myanmar Centre for Responsible Business	Myanmar
Namati	Kenya, Bangladesh, Global
National Democratic Institute	Global
Norwegian Refugee Council	Nigeria, Colombia, Global
NYU Law	Kenya, West Africa
Office of the Episcopal (Anglican) Bishop of Maine	US, Haiti, & the Anglican Communion
Omidyar Network	Global
Open Society Justice Initiative	Global
Politeia	Argentina
Privacy International	Global
Shendi University	Sudan
Socio-Economic Rights & Accountability Project	Nigeria
Statelessness Network Asia Pacific	Asia Pacific
Swathanthra Malayalam Computing	India
The Centre for Internet and Society, New Delhi	India, Estonia, UK, Nigeria, Kenya
The Migration Project	Australia, US, UK, EU
The Nubian Rights Forum	Kenya
The Rockefeller Foundation	Global
University of Abomey-Calavi	Benin
University of Liverpool	Latin America/Caribbean
Unwanted Witness	Uganda

