PRINCIPLES ON IDENTIFICATION

FOR SUSTAINABLE DEVELOPMENT

PRINCIPLES ON IDENTIFICATION FOR SUSTAINABLE DEVELOPMENT:
TOWARD THE DIGITAL AGE

ENDORSING ORGANIZATIONS

African Development Bank

Asian Development Bank (ADB)

Bill & Melinda Gates Foundation (BMGF)

Center for Global Development (CGD)

Digital Impact Alliance (DIAL)

Digital Nations

FHI 360

ID4Africa

International Organization for Migration (IOM)

International Telecommunication Union (ITU)

International Union of Notaries

Mastercard

Norwegian Agency for Development Cooperation (Norad)

Omidyar Network

Open Identity Exchange UK/Europe

Organization of American States

OSCE Office for Democratic Institutions and Human Rights (ODIHR)

Plan International

Privacy and Consumer Advisory Group to the Government Digital Service and GOV.UK

Secure Identity Alliance (SIA)

Smart Africa

The GSMA

UN World Food Programme

UNHCR, The UN Refugee Agency

United Nations Capital Development Fund (UNCDF)

United Nations Children's Fund (UNICEF)

United Nations Development Programme (UNDP)

United Nations Economic Commission for Africa (ECA)

Women in Identity

World Bank Group

PRINCIPLES

INCLUSION

1. **Ensure universal access for individuals, free from discrimination.**
2. **Remove barriers to access and use.**

DESIGN

3. **Establish a trusted—unique, secure, and accurate—identity.**
4. **Create a responsive and interoperable platform.**
5. **Use open standards and prevent vendor and technology lock-in.**
6. **Protect privacy and agency through system design.**
7. **Plan for financial and operational sustainability.**

GOVERNANCE

8. **Protect personal data, maintain cyber security, and safeguard people's rights through a comprehensive legal and regulatory framework.**
9. **Establish clear institutional mandates and accountability.**
10. **Enforce legal and trust frameworks through independent oversight and adjudication of grievances.**

PURPOSE

Every person has the right to participate fully in their society and economy and to be recognized as a person before the law.[1] Yet, as many as 1 billion people across the world do not have basic proof of identity, which is essential for protecting their rights and enabling access to services and opportunities.[2] Many more have forms of identification that are insecure or untrusted by service providers, or live in countries where identification systems are weak and unsuited for the digital era, or fail to safeguard people's rights and data. Addressing this "identification gap"—by improving the coverage, quality, and governance of identification systems that protect rights and facilitate access to services—is, therefore, critical to the development agenda.

The organizations endorsing these Principles are committed to a shared set of values, with the goal of ensuring that identification systems are inclusive, protective of individuals' data and rights, and designed to support development outcomes.

Building on existing international norms,[3] the Principles were first developed and published in 2017 by a group of organizations committed to supporting the development of identification systems that are inclusive, trusted, accountable, and used to enhance people's lives and the achievement of the Sustainable Development Goals (SDGs). Given the quickly evolving nature of the identification sector, the original signatories to the Principles committed to revisiting them to incorporate new perspectives and lessons learned. This second edition reflects inputs from this process and from broader public consultations.

The endorsing organizations—consistent with their respective mandates, operational policies, and rules—use these Principles to promote a common understanding of key issues and good practices; improve stakeholder alignment; guide support and funding decisions; facilitate discussions at country, regional, and/or global levels; and work together to support identification systems that advance economic and social development, protect individual and human rights, and leave no one behind. We hope that a progressively wider range of stakeholders—including governments, intergovernmental organizations, development partners, local and international civil society and nongovernmental organizations, and private sector actors—will join us in endorsing the Principles and putting them into practice.

---

1 The right to recognition before the law is enshrined in Article 6 of the Universal Declaration on Human Rights (UDHR) and Article 16 of the International Covenant on Civil and Political Rights (ICCPR). The right to birth registration is enshrined in several international conventions, including Article 7 of the Convention on the Rights of the Child (CRC).

2 Estimates from the 2018 World Bank Global ID4D Dataset are available at http://id4d.worldbank.org/glo al-dataset

3 This includes, among others, the UN Principles and recommendations on Civil Registration and Vital Statistics (CRVS), international norms on data protection (such as the European General Data Protection Regulation and Council of Europe Convention 108+), global and regional standards and trust frameworks for identification, and the Principles on Digital Development.

Definitions and Scope

These Principles are intended to apply broadly to the creation and use of identification systems[4] to advance development goals. Because of their central role in realizing individual rights and facilitating access to basic services and entitlements in the physical and digital worlds**, the focus of the Principles is on "official" identification systems provided by, on behalf of, or recognized by governments.**[5]

While each country typically has a unique constellation of official identification systems that can differ greatly in their purpose, provider, technology, architecture, use, and governance arrangements, these systems can be broadly categorized as "legal" or "functional" identification systems. **Legal identification systems** provide recognition before the law and proof of legal identity. The name and nature of legal identification systems varies under national law, but typically includes civil registration systems, national identification systems, population registries, and other foundational identification systems.[6] **Functional identification systems** provide official proof of identity and authorization for particular purposes or sectors. This typically includes identification systems that provide voter identification, ration cards, social security numbers, health cards, tax numbers, and more; in some cases these credentials may also be recognized as proof of identity for other purposes or sectors.[7]

Given the overwhelming trend toward digitalization of economies and societies, the Principles reflect the increasingly digital nature of official identification systems. For example, many provide official **digital credentials** and services (such as mobile IDs, digital certificates, e-signatures, etc.) that enable automated and remote authentication for access to services and entitlements, both in person and online. In some cases, governments have built these systems themselves. In others, countries have developed ecosystems of digital identity providers that rely on existing official identification systems for identity proofing and enrollment. Under a federated ecosystem model, for example, multiple public and/or private entities operating within a trust framework can issue officially recognized digital identity credentials. Emerging decentralized identity architectures and standards are also creating possibilities to store and verify official digital credentials on personal devices.

For the remainder of this document, the term "identification system" is used to refer to the analog and digital versions of the official identification systems described above.

---

4 Broadly speaking, identification systems collect and validate identity data through a registration process and then provide people with credentials—such as certificates, cards, or other identity documents—they can use to authenticate themselves or verify specific identity attributes to a third party that needs to rely on their identity or attribute claims.

5 Government recognized ID systems are enabled by and adhere to a country's legal framework, and are based on an identity proofing process that involves validating the holder against government-issued credentials and/or authoritative source registries such as civil registration systems, national identification systems, or population registers.

6 Governments retain ultimate responsibility for legal identification (see, for example, the Official UN Operational Definition of Legal Identity, ECOSOC resolution E/CN.3/2020/15). Although proof of legal identity—particularly birth and/or marriage registration—is frequently a requirement for acquiring a nationality, legal identification need not be linked to nationality and should not be equated with legal or national status. While some legal identification systems (e.g., national identification systems) require or constitute proof of nationality, others do not.

7 In the case of asylum seekers and refugees, although host states are primarily responsible for providing proof of a legal identity for refugees who do not have valid travel documents, the credentials issued by the UN Refugee Agency under its mandate on behalf of the host state can be recognized as proof of legal or official identity (1951 Convention on the Status of Refugees, Articles 25 and 27; 1950 Statute of the Office of the United Nations High Commissioner for Refugees).

Why identification matters for development

For people, identification is a right, an instrument of protection, and a gateway to access services, benefits, and opportunities.

The importance of identification for people's rights and for development was recognized by the international community through adoption of the Sustainable Development Goal (SDG) Target 16.9: "by 2030, provide legal identity for all, including birth registration." The right to an identity starting from birth—as guaranteed in Articles 7 and 8 of the Convention on the Rights of the Child (CRC)—and to be recognized as a person before the law are critical first steps in ensuring lifelong protection and are a prerequisite for exercising other rights. A legal identity is the basis on which children can establish a nationality, avoid the risk of statelessness, and seek protection from violence and exploitation. For example, proof of age is needed to help prevent child labor, child marriage, and underage recruitment into the armed forces.

Furthermore, having an official way to prove one's identity may be requied for many formal interactions, transactions, and services across the public and private sector. For example, verifying a person's identity against an official credential or registry is often required to open a bank account, vote in an election, obtain formal employment, acquire a nationality, register for school, enroll in health insurance, receive a social transfer, buy a SIM card, register property, cross borders, or seek legal redress. The acceleration toward online services and digital transformation across governments and firms means that people also increasingly need a secure and accessible means to prove their identities remotely, such as over the internet.[8]

For governments, private sector actors, and other stakeholders, being able to reliably identify people or verify certain attributes is critical for delivering programs and services efficiently, effectively, and accountably.

The ability to know who people are is essential for a number of government responsibilities, including targeting social programs and ensuring that the correct people receive benefits; responding to emergencies, disasters, and epidemics that require rapid direct assistance; collecting taxes; reducing fraud in public wages; facilitating safe and orderly migration; and, in the case of civil registration, producing vital statistics for planning and monitoring development progress. For certain private entities, verifying customers' identities to a particular level of assurance for certain services—such as opening or allowing access to an account—is necessary to mitigate risk, comply with customer due diligence (CDD) or know your customer (KYC) requirements or

8 For these reasons, identification is a key enabler of numerous SDG targets in addition to 16.9, including 1.3 (implementing social protection systems), 1.4 (ensuring that the poor and vulnerable have control over land, property, and financial assets), 5a (giving poor women equal access to economic resources, including finance), 5b (enhancing the use of technology, including ICT to promote women's empowerment), 8.10 (universal access to banking, insurance, and financial services), 10.7 (safe and responsible migration and mobility), 10c (reducing the cost of remittance transfer), 12c (phasing out harmful fuel subsidies), 16a (strengthening the capacity to fight terrorism and crime), 16.5 (reducing corruption), and many others.

other regulations, and protect clients against identity fraud and theft. When identification systems provide digital mechanisms for individuals to authenticate themselves remotely in online contexts, they are also important enablers of an inclusive digital economy and underpin digital platforms across sectors, including for online services and digital payment systems.[9]

When designed and used appropriately, identification systems have the potential to help countries accelerate inclusive development.

This includes improving governance and service delivery, increasing financial inclusion, reducing gender inequalities by empowering women and girls, and increasing access to health services and social safety nets for the poor. Compared to paper-based registries, the adoption of digital technologies has the potential to increase the accuracy and reliability of identity data and credentials, automate processes to save money and increase convenience, and provide new platforms for innovations in service delivery. Although there are risks to digital technology, digitalization also presents the opportunity to intentionally design identification systems to be more inclusive, user-friendly, and protective of people's rights and data than ever before through the development of new standards, models, and tools to exercise personal oversight and control over how data are used.

---

9 See, for example, FATF. 2020. Guidance on Digital Identity. Financial Action Task Force (FATF), Paris; World Bank. 2018. "Private Sector Economic Impacts from Identification Systems." Washington, DC; Gelb, A., and Metz, A. 2018. *Identification Revolution: Can Digital ID Be Harnessed for Development?* Washington, DC. Center for Global Development; Gelb, A., and Clark, J. 2013. "Identification for Development: The Biometrics Revolution," *Center for Global Development Working Paper 315*.

Why building "good" identification systems is essential to mitigating risks

Despite the opportunities that come with improving identification, identification systems that are poorly implemented or inappropriately used can create a number of risks; these risks disproportionately affect already disadvantaged groups and can be amplified by digital technology.

Key risks include those related to exclusion or discrimination, data protection and privacy, and poorly designed and implemented identification systems that waste resources while offering few benefits. Vulnerable and marginalized groups are often the least likely to have proof of their identity, but also the most in need of the protection and services linked to identification.[10] People who are unable to obtain or easily use identification are therefore at greater risk of being left behind when strict identification requirements must be met to access services. Without proactive mitigation measures, new or upgraded identification systems may reinforce or perpetuate existing inequalities, discriminatory practices, and structural biases. Like other systems that process personal data, identification systems may also undermine individual data protection and privacy rights in the absence of appropriate laws and regulations, oversight, and technical controls and safeguards. Data breaches, unauthorized use or surveillance, identity fraud, and function creep can put people—especially vulnerable groups—at serious risk of harm. Furthermore, identification systems are often built with a "top-down" approach and little transparency. Together with poor procurement practices and design choices that inflate costs and lead to vendor or technology lock-in, this can result in systems that are operationally or financially unsustainable and that do not serve people's needs or development goals.

While these risks are present in any identification system, they may be amplified by digitization. With digital technologies, the potential scale and harm of the mismanagement or misuse of personal data are much greater than with paper-based systems. Similarly, the adoption of technologies that depend on internet connectivity and expensive devices has the potential to widen the digital divide and create new obstacles for already marginalized groups to reliably obtain or use identification. The speed of innovation can also create incentives to focus on obtaining the latest technology rather than building systems that are fit for current purposes and flexible for future needs. Furthermore, even if identification systems are successfully digitized, they are unlikely to reach their potential without full digitalization—transforming and rethinking processes for the digital medium—and complementary investments in internet connectivity, online services, payment platforms, and other digital systems.

---

10 The particular groups most at risk of being excluded by identification systems vary by context, but often include people living in poverty, women and children, migrant populations, refugees and asylum seekers, remote and rural residents, ethnic, linguistic, or religious minorities, sexual and gender minorities, persons with disabilities, the internally displaced, stateless persons, conflict-affected persons, informal sector workers, and other marginalized or minority groups. See, for example, World Bank. 2019. *Global ID Coverage, Barriers, and Use by the Numbers: An In-Depth Look at the 2017 ID4D-Findex Survey*, Washington, DC: World Bank Group.

To harness the benefits of identification systems in the digital era, these risks must be proactively, comprehensively, and continuously addressed by stakeholders.

Building an identification system that meets development goals requires a multifaceted, multi-stakeholder approach. This requires clearly defining the purposes and intended uses of the system; adopting and resourcing adequate legal and regulatory frameworks that remove barriers to access and provide sufficient safeguards and oversight; implementing inclusive policies and practices for identification system enrollment and use; following a people-centric and data privacy–protecting approach for design and risk assessment; and selecting context-appropriate, equitable, and accessible technologies that ensure the quality, security, and utility of the system now and in the future. Continuous and transparent engagement with the public and a diverse set of stakeholders throughout these processes are essential for fostering trust and accountability, and ensuring that identification systems are built to be useful for people and support sustainable development outcomes.

Key Stakeholders and Roles

In practice, applying the Principles requires a coordinated, sustained effort by multiple stakeholders who play essential roles in providing, using, overseeing, and funding official identification systems:

- **Individuals.** People are the center of identification systems, both as the data subjects of these systems and the end-users who rely on identification to protect and claim their rights and to access services. They have the right to know and exercise appropriate oversight and control over how—and for what purpose—their personal data are collected, used, stored, shared, and otherwise processed by public and private bodies. Understanding and responding to people's identification-related needs and concerns, protecting their personal data and privacy, and ensuring their participation in the design and implementation of identification systems that affect their lives are essential.

- **Governments.** National and local government agencies are typically the identity providers for legal identification systems—e.g., civil registration and vital statistics (CRVS), national identification systems, population registries, foundational ID credentials, and so forth—as well as many functional systems, such as voter IDs, tax identifiers, and drivers' licenses. Other government agencies and service providers are frequently relying parties for these systems, using them to identify or authenticate the people they interact with or serve. Government institutions, including legislatures and oversight bodies, also play a critical role in creating and enforcing legal and regulatory frameworks to enable and safeguard identification systems provided by both the public and private sectors. Finally, government agencies are typically involved in setting standards and developing and supervising trust and assurance frameworks for identity providers, relying parties, and other stakeholders in centralized, federated, or decentralized digital identity ecosystems.

- **Private sector.** Private companies are frequent developers, innovators, and suppliers of identification system components and infrastructure, and may also be providers of identity verification and authentication services. Many private companies are also relying parties who depend on legal or other identification systems to verify or authenticate the identities of their customers (e.g., to open bank or mobile money accounts). In some cases, private sector entities are identity providers within a federated or decentralized ecosystem that use government-issued credentials and authoritative source registries (e.g., civil registries and national identification systems) to create digital credentials or authentication services that are accepted for online government (and private sector) services.

- **Nongovernmental, community-based, and civil society organizations.** Nongovernmental organizations (NGOs), civil society and community-based organizations (CSOs and CBOs) can play vital roles in the design and implementation of identification systems, including through advocacy activities, providing protection and legal assistance, spreading awareness, facilitating community consultations, empowering people to access identification or grievance redress mechanisms, and holding identity providers accountable.

- **International organizations, regional bodies, and development partners.** International inter-governmental bodies, development and humanitarian agencies, foundations, and other donors often provide support for identification systems in the form of funding and technical assistance, and support the establishment of normative standards. Other international and regional bodies are also involved in setting standards related to identification, including those for cross-border interoperability and mutual recognition of credentials. In certain cases, development and humanitarian actors may also be identity providers or administer identification systems for specific programs or activities. In the case of refugees and asylum seekers, UNHCR may provide proof of legal or official identity on behalf of the host state under its mandate.

PRINCIPLES

INCLUSION

1 Ensure universal access for individuals, free from discrimination.

- *Legal identity for all.* Everyone should be able to prove their legal identity. Countries must fulfill their obligations and commitments to provide legal identification to all residents[11]—not just citizens[12]—from birth to death, as reflected in international and domestic laws.[13] This includes the obligation of universal birth registration for all children,[14] which is essential for providing proof of legal identity from birth, and the timely registration of other vital events, such as marriages and deaths. It also includes the obligations and commitments to provide proof of legal identity to refugees, stateless persons, and migrants who do not have a valid credential or cannot otherwise prove their legal identity.

- *Nondiscrimination.* All identification systems should be free from discrimination in policy, in practice, and by design. This includes ensuring that legal frameworks; requirements and procedures to register, obtain, or use identification; and the data that are collected or displayed on credentials do not enable or reinforce discrimination against particular groups, such as those who may face increased risks of exclusion for cultural, political, economic or other reasons. Such groups include people living in poverty; women; children; rural populations; racial, ethnic, linguistic, and religious minorities; persons with disabilities; sexual and gender minorities; migrants; asylum seekers, refugees, and the forcibly displaced; and stateless persons among others. Furthermore, identification systems and data should never be used as a tool for discrimination or to infringe on or deny individual or collective rights.

---

11 While states have the sovereign right to determine eligibility for citizenship and issue proof of citizenship in accordance with international law, they also have the obligation to provide proof of legal identity—or recognize legal identification issued by another state or international organization—to all persons resident on their territory, including birth registration. For example, the 1951 Convention on the Status of Refugees, Article 27 provides that States "shall issue identity papers to any refugee in their territory who does not possess a valid travel document," and a similar provision for stateless persons is contained in the 1954 Convention on the Status of Stateless Persons, Article 27. Providing everyone with proof of legal identity is critical to the prevention of statelessness (see www.unhcr.org/ibelong).

12 States should provide proof of citizenship to all persons entitled to it without discrimination of any kind.

13 The obligation of states to provide proof of legal identity does not necessarily mean that enrollment in identification systems should be legally mandatory.

14 For example, Article 7 of the Convention on the Rights of the Child (CRC) states: "The child shall be registered immediately after birth and shall have the right from birth to a name, the right to acquire a nationality and, as far as possible, the right to know and be cared for by his or her parents." The CRC has been ratified by every Member State of the UN except for the United States, which has signed but not ratified the treaty. In practice, however, virtually all births in the United States are registered.

2 Remove barriers to access and use.

- *Direct and indirect costs.* Costs to the individual must never be a barrier to obtain identity credentials required to fulfill rights or access basic services or entitlements. For example, civil registration and the initial issuance of birth and death certificates and other legal identity credentials should be free of charge for the individual. If fees are charged for certain additional services (such as reissuance of lost credentials), rates should be reasonable, proportional to costs incurred, and transparent to the public. The indirect costs of obtaining identification—including fees for supporting documents, travel costs, and cumbersome administrative procedures—must also be minimized.

- *Information asymmetries.* Stakeholders must work to reduce information and knowledge barriers and disparities that might prevent individuals—such as linguistic minorities, people with low literacy levels, persons with disabilities, and others—from accessing or using identification and foster a culture of trust and accountability by increasing literacy and sensitization around the system. Information and education campaigns and other materials must be inclusive and accessible to ensure that everyone has the knowledge, capacity, and tools they need to participate in the identification system and exercise their rights to oversight and control.

- *Technology gaps.* While technology is a key enabler of identification systems, no one should be denied identification or associated services and rights because they lack mobile or internet connectivity, electronic devices, digital literacy or digital skills, the comfort or ability to use certain technology, or because of technology biases or failures. Stakeholders should therefore work together to ensure that identification and authentication services are available and usable for everyone, regardless of digital resources, skills, or connectivity. Furthermore, accessible exception-handling procedures and grievance redress mechanisms are necessary to avoid denial of services or rights and in the case of technical difficulties.

- *Inclusion by design.* Identification systems should prioritize the needs and address the concerns of marginalized and vulnerable groups who are most at risk of being excluded and who are the most in need of the protections and benefits identification can provide. This requires working with communities to proactively identify legal, procedural, social, and economic barriers faced by particular groups, risks and impacts specific to these groups, and adopting appropriate technologies and mitigation measures to ensure that new or updated identification systems do not reinforce or deepen existing inequalities.

DESIGN

3 Establish a trusted—unique, secure, and accurate—identity.

- *Uniqueness.* An identification system provides a mechanism to establish and authenticate a unique identity when—within that system—each person has only one identity and no two people share the same identity. Uniqueness is particularly important within legal identification systems and others that support use cases requiring high levels of assurance,[15] such as government-to-person (G2P) payments and voting. Importantly, uniqueness *within* a given system does ***not*** imply that there must be only one identity provider or system or a single permanent identifier (e.g., a unique ID number) used for all purposes in a country or jurisdiction.

- *Security.* Identification systems must have adequate and effective safeguards against unauthorized access, tampering (alteration or other unauthorized changes to data or credentials), identity theft, misuse of data, cybercrime, and other threats occurring throughout the identification life cycle. Data must be protected at rest and in transit, including when people use their credentials, or including on personal devices. Security measures must include systems to raise awareness about safe utilization of the system and to notify data subjects in the case of data breaches, as well as recourse for identities that have been stolen or compromised and need to be reissued.

- *Accuracy.* Ensuring that identity data are accurate and up-to-date is one of the core principles of data protection and a right of data subjects, and is also essential for the trustworthiness of the system. Identification systems should be designed to ensure accurate data collection and have user-friendly procedures for people to view and update their data and correct errors to ensure accuracy over time.

---

15 Generally speaking, a "level of assurance" (LOA) represents the amount of trust a given identification system or credential provides to a third party that an identity claimed by a person or entity is actually their "true" identity. This is a function of multiple factors, including the strength of the identity proofing process when people are enrolled in an identification system and issued credentials (the identity assurance level or IAL), the strength of the authentication process and technology (authentication assurance level or AAL), and—if using a federated model—the assertion protocol used by the federation to communicate authentication and attribute information (federation assurance level or FAL) (adapted from NIST 800-63:2017).

4 Create a responsive and interoperable platform.

- *Responsiveness.* Identification and authentication services should be designed to meet people's real needs and concerns. In addition, they should be flexible, scalable, and useful for the public agencies and private sector entities that rely on them for identification or authentication. This requires broad stakeholder consultation and a people-centric, participatory approach—including civil society, the public at large, service providers, and other relying parties—beginning with the design process and continuing throughout implementation.

- *Interoperability.* Subject to laws and regulations on data sharing and appropriate technical safeguards, including "privacy-by design" principles, the ability of identification systems to communicate with other systems (e.g., civil registration systems and services providers) and exchange queries or information facilitates services such as identity verification or attestations, eKYC, other permissioned data sharing, and mutual recognition of identification systems across borders.[16]

5 Use open standards and prevent vendor and technology lock-in.

- *Open standards.* Designs based on open standards enable market-based competition and innovation.[17] Open standards are essential for greater efficiency, improved functionality, and adaptability of identification systems, both within countries and across borders.

- *Preventing vendor and technology lock-in.* Good procurement processes facilitate competition, promote innovation, and prevent technology and vendor "lock-in," which can increase costs and reduce flexibility to accommodate changes over time. Procurement processes should emphasize value for money, economy, integrity, fitness for purpose, efficiency, transparency, and fairness. Effective contract management will ensure that these benefits are sustained throughout implementation.

16 Cross-border interoperability can facilitate migration and trade, but controls should be put in place to protect the security of vulnerable groups, such as refugees, whose personal data must often be shielded from their home country.

17 For example, ISO/IEC has developed standards covering many aspects of identification systems. For more, see World Bank. 2016. "Technical Standards for Digital Identity Systems: Formulating a Strategic Approach."

6 Protect privacy and agency through system design.

- *Privacy by design approach.* Identification systems must be designed to prioritize and protect data and privacy as the default setting without requiring any additional special action on the part of an individual. Personal data, including any data that are linked or linkable to an individual, must be protected from improper use proactively and by default through a robust legal and regulatory framework, system design, and the adoption of technical standards and operational controls.[18]

- *Data protection principles in practice.* The design, policies, and technology used by identification systems should comply with global norms for data protection, including data minimization and proportionality, purpose specification, lawful processing, strict limits on data retention, data accuracy, security, accountability, and transparency, among others.[19] For example, identification systems should limit the collection and exposure of data—particularly sensitive personal information[20] —including in credentials and the structure of identification numbers. Authentication protocols must disclose only the minimum data necessary to ensure appropriate levels of assurance and retain data only for as long as required for the purposes for which the data may lawfully be used, or for which consent has been given. These levels and the method of authentication should reflect an assessment of the level of risk in the transactions and should preferably be based on recognized international standards.[21] Data rules and policies should be transparent and made available to people in a user-friendly format to facilitate knowledge of their rights and the processes available to exercise control or oversight of their data.

---

18 On the "privacy-by-design" approach, see, for example, Cavoukian, A. 2011. "Privacy by Design: The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices." https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

19 Commonly referenced examples of standards include the Fair Information Practices (FIPs), the OECD's Privacy Guidelines, the EU's General Data Protection Regulation, the UN Principles on Data Privacy and Protection, and Convention 108+, among others.

20 "Sensitive personal information" can vary by context but commonly includes data that could be used to create fraudulent identities and/or to profile or target individuals. This includes biometric data and identifying numbers, such as permanent or unique identity numbers (UINs), as well as attributes such as religion, ethnicity, caste, political affiliation, and so forth. The disclosure of identifying information may involve particularly serious risks to certain people, for example, asylum seekers and refugees. Therefore, specific considerations apply to ID systems used primarily or exclusively for humanitarian purposes, particularly in settings affected by conflict, violence, and fragility. See, for example, the International Committee of the Red Cross "Policy on the Processing of Biometric Data by the ICRC." 2019. Available at: https://www.icrc.org/en/download/file/106620/icrc_biometrics_policy_adopted_29_august_2019_.pdf, and the ICRC/Brussels Privacy Hub Handbook on Data Protection in Humanitarian Action, 2nd Edition, 2020.

21 Such risk impact assessments should be carried out by the responsible entity that creates, collects, shares, or uses data for authentication and identification purposes linked to the specific use case. Examples of existing standards for levels of assurance for identity proofing include ISO/IEC 29115 and those issued by eIDAS, the UK Cabinet Office, the U.S. National Institute of Standards and Technology (NIST), and others.

7 Plan for financial and operational sustainability.

- *Sustainability.* Identification systems should be designed for long-term fiscal and operational sustainability. This requires a transparent and outcomes-based approach to design to ensure that the system is fit-for-purpose and makes sustainable management and technical choices, and the adoption of business models that ensure the longevity of the system without compromising other Principles. Fees for identification services can create barriers to access, inclusion for individuals, and adoption for service providers. Efforts to recuperate costs through efficiency gains and reduced leakages must also weigh fiscal savings goals against the potential for increasing exclusion errors. Identification systems should be designed to incentivize high standards of performance for all parties involved.

GOVERNANCE

8 Protect personal data, maintain cyber security, and safeguard people's rights through a comprehensive legal and regulatory framework.

- *Legal and regulatory frameworks.* Identification systems must be underpinned by legitimate, comprehensive, and enforceable legal and regulatory frameworks and strong policies that promote trust in the system; ensure data protection and privacy (including cybersecurity); mitigate abuse such as unauthorized surveillance in violation of due process; are free from discrimination and promote inclusion, particularly for vulnerable or marginalized groups; and ensure accountability. Legal frameworks should be clear in delineating liability and recourse for individuals and should be overseen by independent regulatory bodies with appropriate powers and consistent funding. They should also protect people against inappropriate access and use of their data for undue surveillance or unlawful profiling. Frameworks require a balance between regulatory and self-regulatory models that does not stifle competition, innovation, or investment. Appropriate legal and regulatory frameworks are also required for cross-border interoperability or mutual recognition.[22]

- *Rights of data subjects.* Identification services should provide people with genuine choice and control over the collection and use of their data, including the ability to selectively disclose only those attributes that are required for a particular transaction. People should be given a simple means to have inaccurate data corrected free-of-charge and to obtain a copy of their personal data. Personal data should not be used for secondary, unconnected purposes without a person's informed consent, unless otherwise required or authorized under law (for example, as may be necessary and proportionate).[23] Identity providers and other stakeholders should be transparent about identity management; develop appropriate resources to raise people's awareness of how their data will be used; and provide accessible and user-friendly tools to manage their data, provide informed consent, and address grievances. Identity providers should ensure that the initial process to correct errors is administrative rather than judicial in order to increase speed of resolution and reduce costs. Data sharing arrangements should also be transparent and fully documented.

---

22 For example, asylum seekers and refugees must be given special consideration; see *UNHCR Advisory Opinion on the Rules of Confidentiality Regarding Asylum Information* at https://www.refworld.org/docid/42b9190e4.html

23 See, for example, Convention 108+, Articles 5, 10, and 11.

9

Establish clear institutional mandates and accountability.

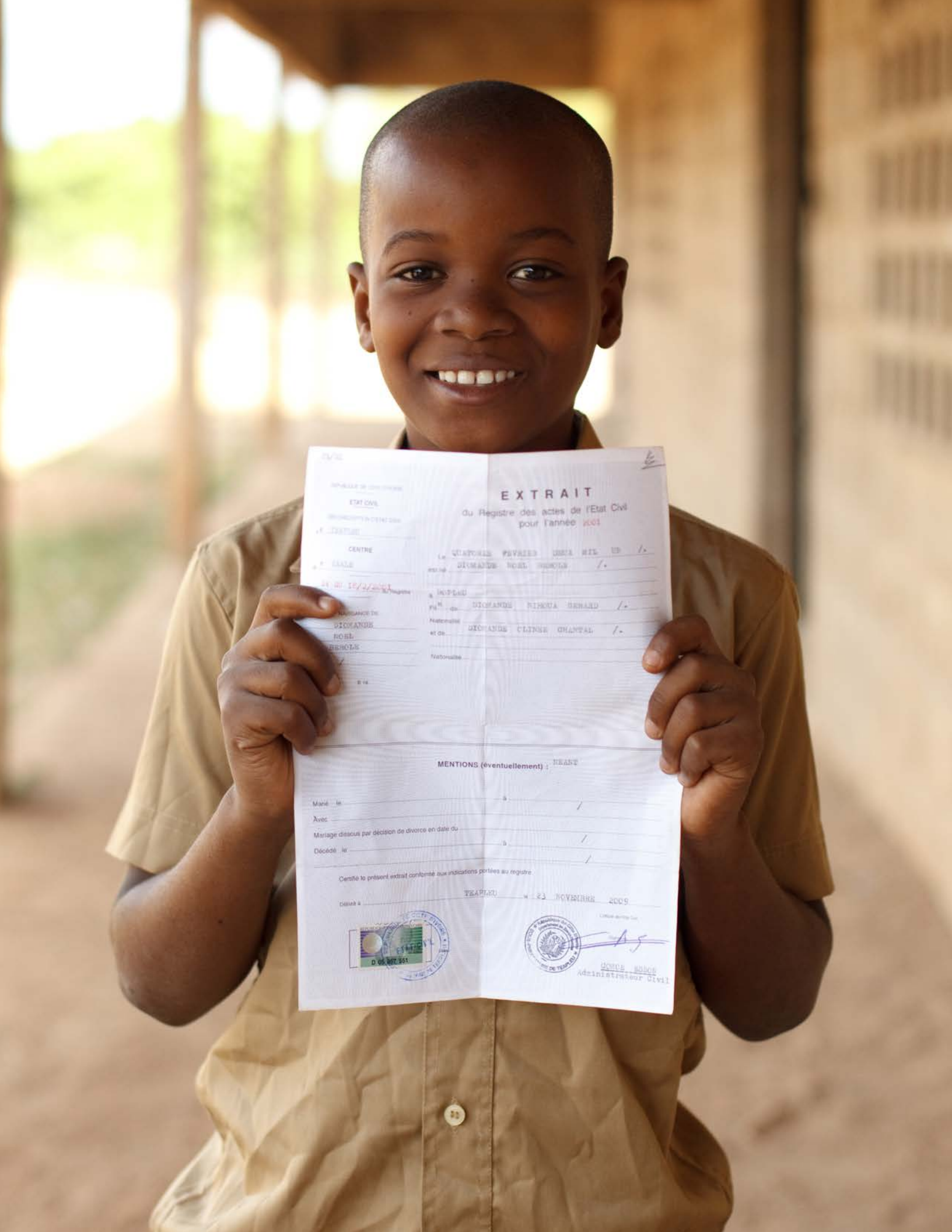
- *Institutional mandates.* Legislation, regulation, and trust frameworks must establish and regulate comprehensive governance arrangements for identification systems and providers domestically and—if applicable—internationally. This should include specifying the terms and conditions governing the institutional relations among participating parties, so that the rights and responsibilities of each are clear to all.
- *Accountability.* There should be clear accountability and transparency around the roles and responsibilities of all entities involved in building, operating, managing, and overseeing identification systems.

10 Enforce legal and trust frameworks through independent oversight and adjudication of grievances.

- *Oversight.* the use of identification systems should be independently monitored (for efficiency, transparency, exclusion, misuse, etc.) to ensure that all stakeholders comply with applicable laws and regulations, appropriately use identification systems to fulfill their intended purposes, monitor and respond to potential data breaches, and receive individual complaints or concerns regarding the processing of personal data. Regulators should be sufficiently resourced and empowered to discharge their statutory responsibilities.

- *Adjudication.* Disputes regarding identification and the use of personal data—for example, refusal to register a person or to correct data, or an unfavorable determination of a person's legal status—that are not satisfactorily resolved by identity providers should be subject to a rapid and low-cost review by independent administrative and judicial authorities with the authority to provide suitable redress without adding barriers for the individual.

Photo Credits | Cover Top: UN Women/Fatma Elzahraa Yassin, Middle: iStock.com/hadynyah, Bottom: iStock.com/borchee; Page 7: UNICEF/BANA2012-02020/Jannatul Mawa; Page 9: iStock.com/ Bartosz Hadyniak; Page 11: Sébastien Rieussec/Safran; Page 15: UN MediaJashim Salam.



EXTRAIT

du Registre des actes de l'Etat Civil
pour l'année 2001

ETAT CIVIL

CENTRE

DIOMANDE
NOEL
NICOLE

MENTIONS (éventuellement) : NEANT

Marié le à /

Avec

Mariage dissous par décision de divorce en date du à /

Décédé le à /

Certifié le présent extrait conforme aux indications portées au registre

Délivré à TEAPLEU le 23 NOVEMBRE 2009

D 05 867 551

Administrateur Civil

ENDORSING ORGANIZATIONS

Empowered lives.
Resilient nations.

We welcome additional organizations to join us in endorsing these Principles

February 2021