

Chapter

10

National Identity System

Why it is important: Everyone has the right to be recognized as a person before the law, as enshrined in Article 6 of the Universal Declaration on Human Rights and several other international human rights instruments. Legal identity is widely recognized to be fundamental to the exercise of human rights and to benefit from numerous government and private sector services. As such, the 2030 Agenda for Sustainable Development, agreed by all UN Member States in September 2015, established a specific target within the Sustainable Development Goals (SDGs) – Target 16.9 – to establish “legal identity for all, including birth registration, by 2030.”¹

¹ United Nations, Principles of Legal Identity in the Context of the 2030 Agenda for Sustainable Development, New York, September 2018, p. 1.

Introduction

This chapter provides best practices for national identification registration and management of a national identification system. A national identification system is a foundational identification system that provides national IDs - often in the form of a card - and potentially other credentials. Foundational ID systems provide general identification and credentials to the population for public administration and a wide variety of public and private sector transactions, services, and derivative credentials.² Foundational ID systems are therefore distinct from functional (sector specific) ID systems, which are created for a particular service or transaction - such as driver and vehicle registration, voting registration, tax administration, and social and transfer programs. Countries may maintain many functional ID systems and issue associated functional identity credentials.³ In addition, there may be privately issued ID credentials. This chapter addresses a country's national identification system, with a focus on the integration of that system with the civil registration system.⁴

This chapter covers the following topics:

1. Agency Responsible for National ID Management, Powers and Responsibilities
2. Accessibility of Services: Location and Powers of ID Registration Offices
3. Universality
4. Enrollment in National ID credential program: Information collected and age of enrollment
5. Validation: Birth Registration as basis for ID registration
6. UIC assignment
7. Process for Information Sharing Between Local Registration Office and National Level
8. Information available from credential
9. Authentication
10. Retirement of Legal Identity
11. Fees and Resources
12. Qualifications of Registrars
13. Process for hearing appeals
14. Monitoring and Evaluation

1. Agency Responsible for National ID Management: Powers and Responsibilities

Best Practice: The legal framework should assign the functions of establishing, operating, and maintaining a national identity management system to a government agency, and provide a clear designation of powers and responsibilities to the relevant agency. In some countries, the agency responsible for ID management is also the agency responsible for civil registration. In other countries, there are different agencies responsible for ID management and civil registration. Either is good practice.

Powers and responsibilities for ID management should include, at a minimum: enrolling individuals in the identity management system (i.e., capturing and recording key attributes, including biographical data and/or biometric data), validating individuals in the identity management system (checking their attributes against existing data to verify identity), issuing identity credentials, and establishing processes for authentication of identity.⁵ The legal framework should empower the head of the national ID management agency, (which we will call the National Identity Registrar) or the Minister in charge of that agency, to set rules and standards for the implementation of various operations within the identity

² ID4D, ID Enabling Environment Assessment, World Bank, 2018, p.9.

³ ID4D, ID Enabling Environment Assessment, World Bank, 2018, p.10.

⁴ For a broader discussion on all types of ID systems, as well a guide to assessing those systems, see ID4D, ID Enabling Environment Assessment, World Bank, 2018, available at: <http://id4d.worldbank.org/legal-assessment>.

⁵ United Nations Guidelines on the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 236

management system, including registration (enrollment and validation) of identity, issuance of identity credentials, management of identity data, and identity authentication services. If the Minister is granted rulemaking authority, rather than the National Identity Registrar, the legal framework should require that the National Identity Registrar be consulted on rule making.

Guidance: Answer the questions below. In the comments section, analyze whether the powers of the national ID management agency and the National Identity Registrar, are adequate to fulfill its responsibilities.

- a. **State which entity is responsible for national ID management** (if part of a ministry, also state the ministry):

Citation:

- b. **Describe the powers and responsibilities of the ID management agency and the National Identity Registrar.** In addition to describing general responsibilities, specifically address if the National Identity Registrar or the Minister has rule-making powers.

Citation:

Comments:

2. Accessibility of Services: Location and Powers of ID Registration Offices

Best Practice: In order to make ID registration accessible to the entire population, ID registration offices should be established at the local level, for example in villages, towns and municipalities. Each primary identity registration office should cover an area that corresponds with minor civil divisions of the country, adjusting boundaries, if necessary, based on population, resources, accessibility, literacy, and simplicity of registration.⁶ In addition, regular daily office hours should be kept.

Duties and responsibilities of local identity registrars should include: collecting biometrics (if applicable) and biographical information; ensuring accuracy and completeness of registration information; validating identity; transferring identity information to the national level; and issuing identity credentials. Because production of the identity credential may require specialized equipment, production of ID cards may be done at the regional or national level instead of the local level. However, a person should not have to travel to the regional or national level to collect an ID card; rather, ID cards should be sent to the local level for issuance or collection.

In some countries, the national identity management agency may also maintain identity management offices that correspond to the major civil sub-divisions of the country. For example, in addition to offices in villages, towns, and municipalities, the national agency may also have offices at the provincial or regional level. These mid-level offices may serve various functions. They may have supervisory authority over the lower-level registration offices in their jurisdiction, be empowered to undertake primary office functions (i.e., identity registration), and/or be responsible for ID credential production. Whether mid-level identity management offices exist, and the powers and responsibilities they hold, is dependent on the needs of the system.

⁶ United Nations, Guidelines on a Legislative Framework for Civil Registration, Vital Statistics, and Identity Management Systems, New York, 2019, Paras. 171 - 173, 239.

Guidance: Describe the location of identity registration offices and, in the comments section, analyze whether identity registration offices and services are reasonably accessible to all persons in the country. Describe the powers and responsibilities of registration offices and, in the comments, note whether each level has sufficient authority to provide efficient service to the population.

- a. **Describe the location of each level of identity registration office.** State whether the location of local registration offices correspond to minor civil divisions, and state the location of mid-level registration offices (if any).

Citation:

Comments:

- b. **Describe the powers and responsibilities of local and mid-level registration offices.** Specifically address whether local and/or mid-level offices are responsible for identity enrollment, identity validation, identity credential production, and identity credential issuance to the individual, or whether some of these responsibilities are assigned only to the national level.

Citation:

Comments:

3. Universality

Best Practice: The ability to prove one's identity is fundamental to the exercise of human rights as well as to benefit from government and private sector services. Therefore, as with civil registration, proof of identity should be provided without discrimination or distinction, including discrimination based on geography; racial, ethnic or religious group; status as a member of a nomadic, indigenous, native or aboriginal population; status as displaced, stateless, refugee, asylum seeker, or person of undetermined nationality; or status as a foreign national born in the country, temporary or migrant worker, or any other immigrant; or any other characteristic. Regardless of the type of identity credential issued, it must be legally valid and be sufficient documentation to gain access to rights and services to which the individual is entitled.⁷

While some form of proof of identity must be available to all, a national identity card or other credential is not necessarily compulsory. Country practices vary on whether registering for and obtaining a national identity card or other credential is mandatory, voluntary, or even available. In countries that do not issue a national identity credential, other forms of identification are issued for sectoral purposes (for example, passport, driver's license, etc.) and can be used as proof of identity.⁸ In all cases, some form of proof of identity should be available to all persons within the territory of a country without discrimination.

Guidance: Describe whether some form of national identity document or credential is compulsory or available for all persons within the country. Consider all forms of discrimination that may take place,

⁷ United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 436.

⁸ United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, Para. 47.

including geography; racial, ethnic or religious groups; nomadic, displaced, native or aboriginal populations; refugees or asylum seekers within the country; foreign nationals born in the country; temporary or migrant workers, or any other immigrant; or any other characteristics. Describe whether different forms of identity documents are provided for different populations (for example, a national ID card for citizens and an immigration card for non-citizens). In the comments section, describe whether the law aligns with best practice and note any recommendations for regulatory reform.

a. Is some form of identity credential available and provided for all, regardless of:

Geography (for example, remote areas)? ☐ Yes ☐ No

Race, ethnicity, religion, gender? ☐ Yes ☐ No

Nomadic, displaced, native or aboriginal population? ☐ Yes ☐ No

Nationality, residency, or refugee/ asylum status? ☐ Yes ☐ No

Other characteristics? ☐ Yes ☐ No

Citation:

Comments:

b. Are different forms of identity documents or credentials provided for different populations?

☐ Yes ☐ No

Citation:

Comments:

4. Enrollment in National ID credential program: Information collected and age of enrollment

Best Practice: Registration for an identity credential entails enrolment in the identity credential system and validation of identity. Enrolment involves capturing and recording key identity attributes from a person who claims a certain identity, which generally includes biographical data (e.g., name, date of birth, sex, etc.), and may include biometrics.⁹

The Information captured at enrollment should be guided by the principle of proportionality and necessity - the principle that personal data should be relevant, limited and adequate to what is necessary in relation to the specified purposes of personal data processing. (See Chapter 10, Data Protection and Personal Privacy). If biometrics are collected, the law should state the type of biometrics collected, including any limitations or constraints on the type of biometrics that may be collected and how they are collected. In addition, because biometrics may be hard to capture on certain individuals (for example, manual laborers or the elderly may have worn fingerprints that cannot be captured clearly and iris scans may be difficult to capture on people with cataracts), there should be back-up measures in place for those individuals whose biometrics cannot be used in the system.¹⁰

There is no best practice for the age of enrollment for a national ID credential. In many countries, particularly those that use biometrics, the age of enrollment is typically between the ages of 15 to 18

⁹ *Technical Standards for Digital Identity*, World Bank, 2017, page 3.

¹⁰ United Nations, *Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems*, New York, 2019, Para. 443 - 446.

years because it has been difficult to reliably capture biometrics on the very young. However, this is changing as biometric technology improves.

Guidance: Describe the biographical information and biometrics, if applicable, captured at enrollment. If biometrics are collected, state any limitations on biometric collection and describe any back-up procedures for individuals whose biometrics cannot be captured or used in the system. State the age of enrollment. In the comments section, describe whether the law aligns with best practice; specifically address whether the information collected aligns with the principle of proportionality and necessity.

a. Information collected (biographical and biometric, including any back-up procedures):

Citation:

Comments:

b. Age of enrollment and procedures for later enrollment:

Citation:

Comments:

5. Validation: Birth Registration as basis for ID registration

Best Practice: Once a person has claimed an identity during ID credential enrolment, their identity is then validated by checking the attributes presented against existing data, including data in the civil register. The validation process ensures that the identity exists (i.e., that the person is alive) and is claimed by one person (i.e., it is unique in the database). In modern digital identity systems, uniqueness is ensured through a deduplication process using biometric data. To ensure that the identity exists, the claimed identity should be checked against data in the civil register.¹¹

The civil register should be the underpinning of a person's civil identification record. If there is no formal linking of the civil register and identity register, there are limited means to confirm the identity of those registered in the national identity system.¹² In addition, national identification systems, which generally enroll people at older ages, cannot ensure that children's rights and services are properly supported through legal identity at birth or provide up to date data on this segment of the population for planning purposes.¹³ Therefore, for those born in the country, proof of birth registration should be required in order to register for a national ID. For those born in the country that lack birth registration, the process of ID credential registration should concurrently facilitate delayed birth registration.¹⁴ If refugees, migrants, stateless persons and other persons born outside the country do not have legally valid birth certificates

¹¹ *Technical Standards for Digital Identity*, World Bank, 2017, page 4.

¹² Principles of Legal Identity in the Context of the 2030 Agenda for Sustainable Development, Working Paper of the Identification for Development Programme – Series 1, United Nations, September 2018, paragraph 10.

¹³ United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 61.

¹⁴ United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 447.

from their country of origin, they should be provided alternative means to validate their identity and obtain identity credentials.¹⁵

Guidance: Describe how identity is validated during identity credential registration. Specifically, state whether proof of birth registration (e.g., a birth certificate) is required in order to register for an identity credential. If a person born in the country lacks birth registration, state whether birth registration is facilitated during identity registration. Describe the process for identity registration for migrants, refugees, asylum seekers, stateless persons and other foreign nationals. In the comments section, describe whether the law aligns with best practice and note any recommendations for regulatory reform.

-
- a. Describe how identity is validated for ID registration (including whether birth registration is required).**

Citation:

Comments:

- b. For those born in the country that lack birth registration, is delayed birth registration facilitated concurrently with ID registration? If yes, describe.**

Citation:

Comments:

- c. For migrants, refugees, asylum seekers, stateless persons and other foreign nationals, what documents are used to validate identity?**

Citation:

Comments:

6. UIC assignment

Best Practice: As discussed in the Birth and Death Registration Chapter, for those born in the country in which a UIC is used, a UIC should be assigned at birth. However, if the assignment of a UIC at birth is a new requirement in a country, many people will have been born before the requirement comes into effect. In addition, there will be people that immigrate into a country. These people will not have had an opportunity to receive a UIC at birth.¹⁶

Therefore, legislation may require all individuals permanently residing within the territorial jurisdiction of the country, who were not previously assigned a UIC, to apply for a UIC by a certain age. For those not

¹⁵ United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 62.

¹⁶ United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 440.

previously assigned a UIC, a UIC may be assigned at the time a person registers for a national ID credential. In countries that use a UIC, a UIC should not be denied based on citizenship, nationality or residency status, as it does not confer citizenship or any specific legal rights.¹⁷

Guidance: For those who have not previously been assigned a UIC, state whether a UIC is assigned during ID credential registration. In the comments section, describe whether the law aligns with best practice and note any recommendations for regulatory reform.

-
- a. **UIC assigned during ID credential registration for those who have not previously been assigned a UIC?** ☐ Yes ☐ No.

Citation:

Comments:

7. Process for Information Sharing Between Local Registration Offices and National Level

Best Practice: Because there will be many identity registration offices throughout the country, there must be clear procedures for transferring information collected by local identity registrars to the central identity register on a regular basis. The legal framework should set timeframes for this transfer of information and steps should be taken to speed up information sharing in order to enable faster processing of identity registration and production of identity credentials.

Guidance: Describe the legal framework related to the transfer of information collected by local identity registrars to the central identity register. In the comments section, note any challenges to the timely and efficient sharing of information.

-
- a. **Describe the process for transfer of information from local identity registrars to the central identity register, including timeliness.**

Citation:

Comments:

8. Information available from credential

Best Practice: Common types of digital identity credentials fall into three categories: 1) something you know (e.g., a password), 2) something you have (e.g., an ID card, mobile phone or a cryptographic key), or 3) something you are (e.g., a fingerprint or other biometric data).¹⁸ Various types of technology may be used with these types of credentials. For example, an ID card may record a digital cryptographic key and/or biometric on an embedded computer chip or may have an encrypted 2D barcode containing a person's personal data and biometrics, either instead of or in addition to a chip. Mobile devices may have

¹⁷ United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 440.

¹⁸ *Technical Standards for Digital Identity*, World Bank, 2017, page 4.

SIM cards with digital certificates. In some cases, identifying information (such as UIC and biometrics) may be stored in the cloud and a physical credential may not be issued.¹⁹

Regardless of the type of credential, it is important that confidential information and information that may make an individual vulnerable to discrimination not be displayed on the face of the credential (in the case of an ID card) or be obtainable from the credential (e.g., chip, SIM technology) by those who have no legitimate interest in the information. Only limited information is necessary on the face of, or available from, the credential, particularly if a credential has biometrics, a PIN, or other authenticating method associated with it.

Because a UIC is used to access services, it should be closely guarded and protections put in place to protect against its unauthorized use. Placing a UIC on the face of an ID credential creates a risk and it is therefore recommended not to place the UIC on the face of ID credential. However, if a UIC is presented on the face of an ID credential, a second type of authentication (such as biometric match) should be required in order to use the UIC.

Guidance: Describe the type of credential and technology used. Describe what information is accessible to individuals and service providers presented with the credential as a form of identity authentication. State whether this information includes confidential or sensitive information. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

a. Credential and technology used:

Citation:

Comments:

b. Information available from the credential (including whether UIC is on the face of the credential):

Citation:

Comments:

9. Authentication

Best practice: Authentication is the process of verifying the claimed identity against the registered identity information;²⁰ in other words, proving a person is who they say they are. Authentication should not be confused with "authorization", which involves determining whether a person has a right to a particular service.²¹

¹⁹ United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 451.

²⁰ *Technology Landscape for Digital Identity*, World Bank, 2018, page 6.

²¹ *Technology Landscape for Digital Identity*, World Bank, 2018, page 7.

Authentication may occur using one or more factors that, like credentials, generally fall into one of three categories—something you know, something you have, something you are.²² Authentication using these attributes can occur through various pathways. For example, a person with a smart card may also need to key in a Personal Identification Number (PIN), or match their fingerprints to those contained in a chip. A person using a mobile phone app may authenticate by use of a PIN, biometrics or a mobile signature. A cloud-based system (like India's Aadhaar system) might rely on biometrics for authentication.²³

All systems are vulnerable to failure. Biometric authentication can sometimes fail to recognize an individual, even though they are who they say they are. A person may forget their PIN. Authentication failure might result in a risk of exclusion from key services. Therefore, no matter what type of authentication process is adopted, there should be alternative authentication procedures in case of authentication failure, such as mobile one-time password (OTP), alternative biometric, or authentication by a local authority.²⁴

Guidance: Describe the authentication process used with a national ID credential. Describe any alternative procedures in case of authentication failure. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

a. Authentication process and alternative procedures in case of authentication failure:

Citation:

Comments:

10. Retirement of Legal Identity

Best practice: Retirement of legal identity - including deactivation of a UIC and identity credential - upon death is important in order to prevent fraudulent use of the deceased's identity. An efficient and effective connection between the civil registration system and the identity management system is the best way to ensure that this deactivation occurs, through the transfer of death record information from the civil registration system to the identity management system. There may be other reasons for deactivation of a UIC or identity credential during a person's life, such as fraudulent use of the identity.²⁵

After deactivation of a UIC and identity credential, identity records should be retained and permanently archived. Country practices vary on the reuse of a UIC after closure. In some countries a UIC is never reused; in others a UIC is not reused for at least 50 to 100 years after the person's death.²⁶

Guidance: Describe whether and how a legal identity (including a national ID credential and UIC, if applicable) is retired upon death and for any other circumstances. Specifically address if there is an obligation for death registration information to be transferred from the civil registration authority to the

²² Other types of information, such as location data or device identity, may be used by a verifier to evaluate the risk in a claimed identity, but they are not considered authentication factors. Grassi, P., et. al, NIST Special Publication 800-63-3, *Digital Identity Guidelines*, page 12.

²³ United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 461.

²⁴ United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 462-463.

²⁵ United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 464.

²⁶ United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para 465.

national identity management system. In the comments section, describe whether the law aligns with best practice and note any recommendations for regulatory reform.

a. Process and circumstances for retiring a legal identity (including UIC and ID credential):

Citation:

Comments:

11. Fees and Resources

Best practice: There is no best practice regarding charging a fee for identity credential registration and credential issuance. Many countries charge a fee. However, if obtaining an identity credential is mandatory or essential for individuals to benefit from basic services, policy makers should consider providing the original identity credential free of charge or for a minimal fee. In addition, there should be a process for a fee waiver for those who cannot afford the fee. Fees may be charged to replace a lost identity credential.²⁷

Public and private sector entities benefit from the authentication services provided by the identity management system. Therefore, some countries charge a fee to these entities for authentication services. Country policies vary on whether to charge government entities - such as the health care system, social services, and others - a fee for authentication services. In some countries, the identity management authority charges other government entities a fee for this service. In other countries, there is a policy of providing this service to other government entities free of charge. Private institutions, such as banks, that wish to use the identity management system authentication services generally are charged a fee.²⁸

Any revenue generated by the identity management system should be retained to fund the system rather than going to the central treasury.²⁹

Guidance: State the amount of fees charged to individuals for issuance of an identity credential, including fees for an original, renewal and duplicate credential. State the amount of fees charged to institutional users of authentication services, including government and private sector entities. State whether fees generated by the identity management system are retained to fund the system. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

a. Fees charged to individuals for ID credential issuance (original, renewal, duplicate):

Citation:

Comments:

²⁷ United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para 467.

²⁸ United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 468.

²⁹ United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 211.

b. Fees charged to government and private sector users of authentication services:

Citation:

Comments:

c. Is revenue generated by the identity management system retained to fund the system?

Citation:

Comments:

12. Qualifications of Registrars

Best Practice: The National Identity Registrar and local identity registrars hold significant power in validating and assigning legal identity through identity registration and retiring legal identity upon notification of death registration. Registrars may also collect fees, which may make them vulnerable to allegations of corruption. Therefore, it is important that there is a strong legal framework that governs the selection or appointment, qualifications, and proper conduct of identity registrars. To help ensure that ID services are provided in a professional manner, identity registrars should be adequately paid, full-time officials, who enjoy civil-service or public-service status, and are subject to the rules of conduct for civil or public servants.³⁰

Guidance: Describe the legal framework related to identity registrars' selection or appointment, qualifications, and civil or public service status. These requirements are often contained in civil servant laws, regulations or policies. In the comments section, describe whether the law aligns with best practice and note any recommendations for regulatory reform.

a. Describe the required qualifications, and appointment or selection process, for the National Identity Registrar.

Citation:

Comments:

b. Describe required the qualifications, and appointment or selection process, for local identity registrars.

Citation:

Comments:

c. Describe any rules governing proper conduct of identity registrars.

³⁰ United Nations, Guidelines on Legislative Framework for Civil Registration, Vital Statistics, and Identity Managements Systems, New York, 2019, Para. 242.

Citation:

Comments:

d. Are identity registrars full-time and adequately paid, and have civil or public servant status?

Citation:

Comments:

13. Process for hearing appeals

Best Practice: Decisions made by identity registrars can have legal consequences that may fundamentally impact a person's life. Reasonable minds may disagree about how to resolve certain difficult situations and therefore decisions made by identity registrars should be subject to administrative and judicial review. In many countries, before appealing to the courts, an individual must appeal a local official's decision to a higher administrative level, on up to the central level. This is referred to as "exhaustion of remedies" and serves two purposes. First, it allows the ID management agency the opportunity to correct the mistake without burdening the courts. Second, it creates a record of the administrative decision for the court to review. After appealing through administrative channels, up to the central level, an individual should be able to appeal to the courts if they feel they have not been able to obtain a satisfactory resolution of their issue. The legal framework should provide the right to appeal a decision by an identity registrar, a clear process by which to appeal, and time frames in which to appeal.³¹

Guidance: Describe any right to appeal the decision of an identity registrar, including the process by which and the authority to which a person may appeal, and the timeframe for appeal. In the comments section, describe whether the law aligns with best practice and note any recommendations for regulatory reform.

a. Is there a right to appeal the decision of an identity registrar? _____ yes _____ no

Citation:

Comments:

b. Must administrative remedies be exhausted before an appeal is filed in court?

_____ yes _____ no

Citation:

Comments:

c. Describe the appeal process and time frames.

³¹ United Nations, Guidelines on the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 528-530.

Citation:
Comments:

14. Monitoring and Evaluation

Best Practice: A performance-monitoring program is an integral part of identity management systems. Routine monitoring and inspection of an identity registrar's work is required in order to continue to improve the efficiency, effectiveness and quality of the systems.³² There should be a requirement that primary-level identity registration offices be routinely monitored and inspected, either by the central level authority or a mid-level office with supervisory power. If non-conformance to procedures is found, there should be protocols to improve performance, including additional training, warnings, and penalties for poor performance and failure to carry out duties, as well as incentives to encourage local registrars to fulfill their duties.³³ There should be clear procedures and penalties for instances of deliberate misconduct by identity registrars, including fraudulent registrations or inappropriate disclosures.³⁴

Guidance: Describe procedures to monitor and inspect identity registration offices; procedures for correcting poor performance and failure to carry out duties, and procedures for penalizing deliberate misconduct by identity registrars, as well as any incentives to improve the performance of registrars. In the comments section, describe whether the law aligns with best practice and note any recommendations for regulatory reform.

a. Describe any routine monitoring and inspection procedures for identity registration offices.

Citation:
Comments:

b. Describe any procedures for correcting poor performance and/or penalizing misconduct by identity registrars.

Citation:
Comments:

c. Describe any other incentives to improve performance for identity registrars.

Citation:

³² United Nations, Principles and Recommendations for a Vital Statistics System, Revision 3, New York, 2014. Para. 335; United Nations Guidelines for the Legislative Framework for Civil Registration, Vital Statistics, and Identity Management Systems, New York, 2019, Paras. 524-525.

³³ United Nations, Principles and Recommendations for a Vital Statistics System, Revision 3, New York, 2014. Paras. 338-339; United Nations Guidelines for the Legislative Framework for Civil Registration, Vital Statistics, and Identity Management Systems, New York, 2019, Paras. 524-525.

³⁴ United Nations, Principles and Recommendations for a Vital Statistics System, Revision 3, New York, 2014. Para. 326; United Nations Guidelines for the Legislative Framework for Civil Registration, Vital Statistics, and Identity Management Systems, New York, 2019, Paras. 531.

Comments:

