NATIONAL IDENTIFICATION BILL, 2026 (BELIZE)

INDEX / ARRANGEMENT OF SECTIONS

PART IV – REGISTRATION AND ENROLMENT

PART V – IDENTITY DATA AND BIOMETRICS

PART VI – VERIFICATION AND AUTHENTICATION

PART VII – AGENCY AND PRIVATE SECTOR RELIANCE

PART I – PRELIMINARY

1. Short title and commencement

1. This Act may be cited as the **National Identification Act, 2026**.
2. This Act shall come into force on a date appointed by the Minister by Order published in the Gazette.
3. Different provisions of this Act may be brought into force on different dates.

2. Objects and guiding principles

1. The objects of this Act are to—
   (a) establish a secure, inclusive, and trusted framework for civil and administrative identity in Belize;
   (b) facilitate access to public and private services while preventing exclusion, discrimination, or undue hardship;
   (c) ensure that identity and biometric data are processed lawfully, fairly, proportionately, and securely;
   (d) preserve the primacy of civil registration and legal status determination under written law;
   (e) protect the dignity, autonomy, and rights of individuals in the use of identity systems; and
   (f) promote transparency, accountability, and public trust in identity governance.
2. This Act shall be interpreted and applied in accordance with the following guiding principles—
   (a) **lawfulness and necessity**: identity data shall be collected and used only where authorised by law and necessary for a legitimate purpose;
   (b) **proportionality**: the means used to establish or verify identity shall be proportionate to the purpose pursued and the risks involved;
   (c) **non-exclusion**: no person shall be excluded from services or social participation solely by reason of enrolment status, technical failure, or inability to meet identity requirements where lawful alternatives exist;
   (d) **human dignity and autonomy**: the System shall respect the inherent dignity of individuals and shall not reduce identity to a purely technical or automated determination;
   (e) **accountability and oversight**: all actors operating under this Act shall be subject to independent oversight and effective remedies.

3. Interpretation

1. In this Act, unless the context otherwise requires—

   "authentication" means the process of verifying that a person is the legitimate holder or authorised user of an identity credential issued or recognised under this Act;

"Authority" means the National Identification Authority established under section 16;

"authorised operator" means a natural or legal person authorised by the Authority under this Act or regulations to collect, process, verify, or authenticate identity or biometric data on behalf of the Authority or within the System;

"biometric data" means personal data resulting from specific technical processing relating to the physical or physiological characteristics of a natural person that allow or confirm unique identification;

"civil registration" has the meaning assigned under the Civil Registry and Vital Statistics Act, 2025;

"Data Protection Act" means the Data Protection Act, 2021 (Act No. 30 of 2021), and includes any amendment, re-enactment, or replacement thereof;

"**high risk**" in relation to an incident involving identity or biometric data, means a risk of significant harm to the rights, freedoms, security, or lawful interests of an individual, including risk of identity theft, discrimination, exclusion, financial loss, or other serious adverse effect;

"identity data" means demographic, biographic, or biometric data processed for the purposes of this Act;

"**level of assurance**" means the degree of confidence in the accuracy and reliability of an identity verification or authentication process, as prescribed by regulations or technical directions, having regard to the risks and potential impact of the transaction concerned;

"Minister" means the Minister responsible for digital governance;

"Population Register" means the register established under section 10;

"public authority" includes any ministry, department, statutory body, or other entity performing a public function;

"**relying party**" means a public authority or private entity authorised under this Act to obtain verification or authentication services from the Authority for a specified lawful purpose;

"System" means the National Digital Identification System established under section 8;

"Unique Identification Number" or **"UIN"** means the identifier assigned under section 11A and 12.

"verification service" means a controlled query made through authorised interfaces to confirm whether identity data presented corresponds with a record in the System and meets a prescribed level of assurance.

2. A reference in this Act to the "processing" of identity data includes the collection, recording, storage, retrieval, use, disclosure, transmission, verification, or deletion of such data.

4. Application and scope

1. This Act applies to—
   (a) the establishment and operation of the National Digital Identification System;
   (b) the processing of identity data for the purposes of that System; and
   (c) all public authorities, authorised operators, and relying parties acting under this Act.
2. This Act does not apply to—
   (a) the determination of citizenship, nationality, residency, or any civil status; or
   (b) law enforcement, national security, or intelligence activities, except where expressly authorised by written law.
3. Nothing in this Act shall be construed as requiring any person to enrol in the System as a condition of legal existence, dignity, or access to emergency or essential public services.

5. Relationship with civil registration and other laws

1. Civil registration records maintained under the Civil Registry and Vital Statistics Act, 2025 are the sole and authoritative source of civil status, including birth, death, marriage, adoption, and any other matter of legal status provided that nationality status shall be determined and administered by the Ministry responsible for immigration.
2. Nothing in this Act—
   (a) creates, amends, extinguishes, or determines civil status;
   (b) substitutes for civil registration; or
   (c) authorises the Authority to adjudicate disputes relating to civil registration.
3. In the event of any inconsistency between the System or the Population Register and civil registration records, the civil registration record shall prevail.

6. Relationship with data protection law

1. This Act shall be read and applied consistently with applicable data protection legislation.
2. Nothing in this Act limits or derogates from the rights of individuals under the Data Protection Act, including rights relating to access, correction, objection, complaint, or redress.
3. Where a provision of this Act provides greater protection to individuals than the Data Protection Act, the provision affording greater protection shall apply.

7. Nature and limits of identity under this Act

1. Identity established, recorded, verified, or authenticated under this Act is administrative in nature.
2. A record, identifier, verification result, or authentication response generated under this Act—
   (a) does not, of itself, constitute legal proof of identity, civil status, entitlement, or eligibility; and
   (b) shall not be treated as determinative for any purpose unless expressly provided by written law.
3. Nothing in this Act authorises the System or any automated or technical process to determine legal status or rights independently of lawful human decision-making.

PART II – NATIONAL DIGITAL IDENTIFICATION SYSTEM

8. Establishment of the National Digital Identification System

1. There is hereby established a system to be known as the **National Digital Identification System**.
2. The System is established for the purpose of—
   (a) assigning and managing unique administrative identifiers;
   (b) facilitating secure verification and authentication of identity claims in accordance with this Act; and
   (c) supporting access to services in a manner consistent with non-exclusion, proportionality, and human dignity.
3. The System shall operate as a **civil and administrative identity system** and shall not be used as a system of population control, surveillance, or social monitoring.

9. Components of the System

1. The System shall comprise—
   (a) a **Population Register** established under section 10;
   (b) a **Unique Identification Number system**;
   (c) verification and authentication services;
   (d) secure technical infrastructure and audit mechanisms; and
   (e) such ancillary components as may be prescribed by regulations, consistent with this Act.
2. No component of the System may be established or operated except in accordance with this Act and regulations made hereunder.
3. The inclusion of a component in the System does not, of itself, authorise the collection or use of any category of identity data beyond what is expressly permitted under this Act.

10. Population Register

1. There is established a National Identity Register (hereinafter referred to as the "Population Register").
2. The Population Register shall contain prescribed identity data derived from—

   (a) enrolment processes under this Act;
   (b) civil registration records transmitted in accordance with section 11; and
   (c) such other authoritative public sources as may be prescribed by regulations,

   provided that such data is necessary and proportionate for the purposes of this Act.

3. The Population Register—

   (a) is an **administrative register** established solely for the purposes of identity management, credential issuance, and the facilitation of public and private service delivery;

   (b) does not constitute a civil register and **shall not be used to create, confer, or determine civil status**, which remains the exclusive domain of the Civil Registry and Vital Statistics Act, 2025;

   (c) shall not replace, duplicate, or subsume any register maintained under the Civil Registry and Vital Statistics Act, 2025, provided that:

      (i) the Register may **digitally verify** information against civil records; and

      (ii) any data stored from such records shall be limited to the minimum attributes necessary for identity verification in accordance with the principle of **data minimisation**;

   (d) shall, to the greatest extent practicable, implement the **"Once-Only" principle**, obtaining and reusing data directly from authoritative public sources to ensure that individuals are not required to resubmit information already lawfully held by the State.

4. The Population Register shall not contain—
   (a) determinations of citizenship, nationality, or immigration status;
   (b) legal conclusions regarding entitlement or eligibility; or
   (c) any data prohibited under this Act or regulations.

10A. Continuous maintenance of the Population Register

1. The Authority shall implement procedures for the continuous maintenance, reconciliation, and deduplication of the Population Register.
2. Such procedures shall include—

   (a) periodic reconciliation with civil registration records;
   (b) validation against prescribed authoritative sources; and
   (c) audit mechanisms to detect and correct inconsistencies or duplicate records.

3. No individual shall suffer adverse consequences solely by reason of a discrepancy identified during reconciliation.

11. Relationship between the Population Register and civil registration

1. Civil registration records maintained under the Civil Registry and Vital Statistics Act, 2025 remain the authoritative source for civil status.
2. Information from civil registration records may be referenced or verified for the purposes of enrolment or updating the Population Register, in accordance with this Act and regulations.
3. Notwithstanding any provision of this Part, the Civil Registry remains the foundational source of truth for legal status. The System shall be the authoritative mechanism for the verification and authentication of that status through biographic and biometric data.
4. Nothing in this Act authorises the Authority to amend, override, or adjudicate civil registration records.
5. Without prejudice to the primacy of civil registration under the Civil Registry and Vital Statistics Act, 2025, the Authority shall, **in collaboration** with the Civil Registry Department, establish and maintain **interoperability frameworks** and appropriate legal, technical, and institutional arrangements to ensure the systematic, secure, and timely transmission of information relating to births, deaths, and other prescribed vital events to the Population Register for the purposes of—
   (a) **foundational enrolment**, by initiating or updating identity records upon the occurrence of a vital event;
   (b) maintaining the **real-time accuracy** and integrity of the Population Register; and
   (c) ensuring the **automatic deactivation** of credentials or records relating to deceased persons to prevent identity fraud or duplication.

11A. Assignment of Unique Identification Number at birth

1. Upon the registration of a birth under the Civil Registry and Vital Statistics Act, 2025, the Authority shall, through secure interoperability arrangements with the Civil Registry Department, assign a Unique Identification Number to the individual concerned**.**

2. Registration under subsection (1)—
(a) shall not require biometric capture at the time of birth registration;
(b) shall be completed progressively over the individual's lifecycle**,** in accordance with regulations and applicable safeguards; and
(c) shall not, of itself, determine citizenship, nationality, or any civil status.

3. Enrolment in the System and activation of the corresponding Population Register record shall occur in accordance with this Act when the individual, or a person acting on their behalf, applies for enrolment.

4. Regulations may prescribe procedures for deferred, assisted, or representative enrolment of children.

5. The reservation of a Unique Identification Number under this section shall not, of itself, create an active record in the Population Register until enrolment occurs in accordance with this Act.

12. Unique Identification Number

1. Every individual shall have a single Unique Identification Number under this Act.
2. A Unique Identification Number shall be—
   (a) assigned at birth in accordance with section 11A; or
   (b) assigned upon enrolment where no prior Unique Identification Number has been issued.
3. A Unique Identification Number—
   (a) shall be unique and persistent;
   (b) shall not encode personal, biometric, or status information; and
   (c) shall be generated and managed in accordance with security standards prescribed by the Authority.
4. A Unique Identification Number assigned at birth remains reserved until activation through enrolment in accordance with this Act.
5. A Unique Identification Number shall not be reassigned, altered, or duplicated.

13. Updating, suspension, and deactivation of records

1. The Authority shall establish procedures, by regulations, for—
   (a) updating identity data in the Population Register;
   (b) suspending or deactivating records where necessary for accuracy, security, or integrity; and
   (c) recording deaths or permanent departures, without prejudice to civil registration processes.
2. Suspension or deactivation of a record—
   (a) shall not, of itself, result in denial of lawful services;
   (b) shall be proportionate and subject to review; and
   (c) shall not be used as a punitive or coercive measure.

3. Individuals shall have the right to be informed of, and seek review of, any suspension or deactivation affecting their record.

13A. Continuous registration

1. Where an individual is enrolled in the System, the Authority shall maintain a continuous administrative identity record linked to that individual's Unique Identification Number until death or lawful deactivation.
2. A Unique Identification Number assigned at birth under section 11A remains reserved until enrolment and does not, of itself, create an active Population Register record.
3. Nothing in this section shall be construed as requiring any person to enrol in the System.
4. The Authority shall ensure that, once activated, an identity record is maintained in a manner that preserves accuracy, integrity, and lifecycle continuity.

14. Nature and legal effect of System records

1. The administrative and non-determinative character of System records is governed by section 7.
2. No public authority or private relying party shall treat a System response as determinative of a person's rights or obligations unless expressly authorised by written law.
3. The use of System responses shall be subject to the safeguards, fallback procedures, and review mechanisms provided under this Act and regulations.

15. Prohibition on function creep

1. The System shall not be used for—
   (a) mass surveillance, tracking, or monitoring of individuals;
   (b) social scoring, ranking, or behavioural assessment;
   (c) predictive profiling or population analytics unrelated to identity verification; or
   (d) any purpose not expressly authorised under this Act;
2. Notwithstanding subsection (1), aggregated, anonymised, or de-identified data may be used or shared for statistical, research, or public policy purposes, in accordance with applicable law and subject to appropriate safeguards.
3. Any proposal to materially expand the functions of the System shall require—
   (a) express authorisation by Act of Parliament; and
   (b) public consultation and impact assessment as prescribed.

PART III – GOVERNANCE AND INSTITUTIONAL ARRANGEMENTS

16. Establishment of the National Identification Authority

1. There is established a body corporate to be known as the **National Identification Authority**.
2. The Authority—
   (a) shall have perpetual succession and a common seal;
   (b) may sue and be sued in its own name; and
   (c) shall, for the purposes of this Act, be independent in the exercise of its functions, subject to this Act and oversight by Parliament.
3. The Authority shall be independent in the performance of its functions and shall not be subject to the direction or control of any person or authority in relation to
   (a) individual registration decisions;
   (b) data access determinations;
   (c) enforcement or sanctioning actions;
   (d) authorisation or suspension of relying parties; or
   (e) technical standards relating to identity or biometric processing.
4. The Minister may issue general policy directions consistent with this Act, but no such direction shall relate to specific cases, enforcement actions, or operational determinations.
5. Any policy direction issued under subsection (4) shall be published and laid before the National Assembly.

16A. Financial autonomy

The Authority shall prepare and submit its budget estimates in accordance with applicable public finance law.

Funds appropriated to the Authority by the National Assembly shall be applied solely for the purposes of this Act and shall not be subject to direction in relation to operational or enforcement decisions.

The Authority may retain administrative fees prescribed under this Act for the purposes of system maintenance and oversight, subject to financial audit.

17. Functions of the Authority

1. The functions of the Authority are to—
   (a) establish, administer, and maintain the National Digital Identification System and Population Register;
   (b) assign and manage Unique Identification Numbers;
   (c) prescribe and enforce technical standards, security safeguards, and operational

requirements;
(d) approve biometric modalities, devices, and operators in accordance with this Act;
(e) provide verification and authentication services to authorised relying parties;
(f) ensure accessibility, inclusion, and non-exclusion in enrolment and use of the System;
(g) monitor compliance with this Act and regulations; and
(h) protect the rights and interests of individuals whose identity data is processed under this Act.

2. In performing its functions, the Authority shall have regard to—
(a) the guiding principles set out in section 2;
(b) the need to minimise data collection and processing;
(c) the risks of exclusion, discrimination, or harm; and
(d) applicable data protection principles under the Data Protection Act.

3. The Authority may enter into operational arrangements with the Ministry responsible for foreign affairs and with Belize diplomatic missions or consular posts for the purposes of—
(a) facilitating the enrolment of Belizean citizens residing outside Belize;
(b) supporting the collection of biometric and enrolment information abroad;
(c) assisting with the issuance or delivery of National Identification Cards; and
(d) promoting awareness and outreach relating to the National Identification System.

4. The Authority may designate diplomatic missions or consular posts as authorised enrolment locations or credential distribution points in accordance with this Act and regulations made under it.

18. Powers of the Authority

1. The Authority may—
(a) issue binding technical directions, standards, and codes of practice;
(b) accredit, suspend, or revoke the authorisation of biometric operators and relying parties;
(c) conduct inspections, audits, and compliance reviews;
(d) require the production of information reasonably necessary for the performance of its functions;
(e) take remedial or corrective measures in response to identified risks or non-compliance; and
(f) do all things reasonably necessary for carrying out this Act.

2. The Authority shall not exercise its powers in a manner that—
(a) circumvents or substitutes for civil registration processes;
(b) determines legal status or entitlement; or
(c) permits secondary or unauthorised use of identity or biometric data.

19. Board of the Authority

1. The Authority shall be governed by a Board consisting of—
   (a) a Chairperson; and
   (b) not fewer than four nor more than six other members.
2. Members of the Board shall be appointed by the Minister, **subject to a two-thirds majority confirmation by the National Assembly**, from among persons recommended by an **Independent Selection Committee**.
3. The Independent Selection Committee shall be composed of:
   (a) a representative of the Judicial and Legal Services Commission;
   (b) a representative of the Public Service Commission; and
   (c) [one other non-political body, e.g., a Dean of University or Bar Association head].
4. The Committee shall identify candidates through a **transparent, public, and merit-based selection process**, ensuring that appointees possess proven integrity and significant expertise in:
   (a) law or constitutional affairs;
   (b) information security, digital systems, or data protection;
   (c) public administration or digital governance; or
   (d) human rights, social inclusion, or privacy advocacy.

5. A person is disqualified from appointment to the Board if that person—
   (a) holds elected political office;
   (b) is an officer or employee of a political party; or
   (c) has a material conflict of interest relating to the functions of the Authority.
6. In appointing members of the Board, the Minister shall have regard to the need to prevent concentration of representation from entities subject to regulation under this Act.

20. Tenure, removal, and conflict of interest

1. A member of the Board shall hold office for a term of not less than three and not more than five years and is eligible for reappointment once.
2. A member may be removed from office only for—
   (a) inability to perform the functions of office;
   (b) serious misconduct or breach of duty; or
   (c) proven conflict of interest,
   and only in accordance with a procedure prescribed by law.
3. Members of the Board shall—
   (a) disclose any actual or potential conflict of interest; and
   (b) recuse themselves from any matter in which such conflict arises.
4. A member of the Board or senior officer of the Authority shall not, within two years of leaving office, accept employment or remuneration from a relying party or authorised operator regulated under this Act without approval of an independent ethics body prescribed by regulations.

21. Chief Executive Officer and staff

1. The Board shall appoint a Chief Executive Officer of the Authority on such terms and conditions as may be approved by the Minister.
2. The Chief Executive Officer—
   (a) is responsible for the day-to-day administration of the Authority;
   (b) shall not hold elected political office; and
   (c) shall act independently in operational matters.
3. The Authority may appoint such officers and employees as are necessary for the performance of its functions.

22. Advisory and ethics committees

1. The Authority shall establish one or more advisory committees, including—
   (a) an **Ethics and Inclusion Committee**; and
   (b) a **Technology and Security Advisory Committee**.
2. Advisory committees shall—
   (a) include representation from civil society, disability organisations, and technical experts;
   (b) provide non-binding advice to the Authority; and
   (c) operate transparently in accordance with procedures prescribed by the Authority.

22A. Inter-agency coordination mechanism

1. The Authority shall establish and maintain a formal inter-agency coordination mechanism for the purposes of—

   (a) ensuring alignment between the National Digital Identification System and civil registration, immigration, social security, elections, and other prescribed systems;
   (b) facilitating lawful and secure data exchange; and
   (c) resolving operational or governance issues relating to identity management.

2. The coordination mechanism shall include representatives of—

   (a) the Civil Registry Department;
   (b) the Immigration and Nationality Department;
   (c) the Social Security Board;
   (d) the Elections and Boundaries Department; and
   (e) such other public authorities as may be prescribed.

3. The coordination mechanism shall not exercise decision-making authority over civil status determinations or functions vested by law in any participating entity.

23. Transparency and reporting

1. The Authority shall, within six months after the end of each financial year, submit to the Minister and lay before the National Assembly an annual report containing—
   (a) a description of the activities of the Authority;
   (b) information on enrolment, verification, and system use;
   (c) summaries of audits, incidents, and corrective actions; and
   (d) measures taken to promote inclusion and protect rights.
2. The Authority shall publish—
   (a) technical standards and directions;
   (b) codes of practice; and
   (c) non-sensitive audit summaries,
   in such manner as to promote public transparency and trust.

24. Independent and concurrent oversight

1. The Authority shall be subject to oversight by—
   (a) Parliament;
   (b) the Auditor General; and
   (c) the Data Protection Commissioner.
2. Each oversight body shall exercise its powers independently and within the scope of its statutory mandate.
3. Findings, recommendations, or directions issued by an oversight body shall be binding to the extent authorised under that body's enabling legislation.
4. Nothing in this Act confers on one oversight body authority to override or substitute the lawful determinations of another acting within its mandate.
5. Oversight bodies shall, where appropriate, coordinate investigations and share information to avoid duplication and ensure coherent supervisory outcomes.

PART IV – REGISTRATION AND ENROLMENT

25. Eligibility for enrolment

1. Every person lawfully present in Belize is eligible to apply for enrolment in the National Digital Identification System in accordance with this Act and regulations made thereunder.
2. Eligibility for enrolment under this Act—
   (a) shall not depend exclusively on the possession of a prior identity document, and the absence of such a document shall not, by itself, preclude enrolment where identity may be established through any lawful means prescribed under this Act or regulations.

   (b) shall not confer citizenship, nationality, permanent residence, or any civil status; and

(c) shall not be interpreted as a determination of legal status under any other written law.

3. For the purposes of enrolment, supporting documentation may include civil registration records, including birth certificates, as well as documents issued by the authority responsible for immigration or other prescribed sources, in accordance with regulations.
4. A person lawfully present in Belize includes citizens, permanent residents, and other persons authorised to reside in Belize under applicable immigration law, and enrolment of such persons shall be carried out in accordance with procedures prescribed by regulations, including—
   (a) the types of supporting documentation that may be accepted;
   (b) the categories or forms of identity credentials that may be issued, which may distinguish between citizens and different categories of non-citizens; and
   (c) the manner in which status information, where relevant, may be recorded or verified, without conferring or determining such status under this Act.
5. No person shall be refused enrolment solely on the basis of—
   (a) poverty, disability, age, literacy, or geographic location;
   (b) lack of connectivity or access to digital services; or
   (c) inability to immediately satisfy documentary or biometric requirements, where alternative lawful procedures are available.
6. No person shall be refused enrolment solely on the basis of naming conventions, absence of a surname, cultural naming structures, or lawful religious objections to particular technical processes, provided that alternative procedures prescribed by regulations are satisfied.
7. The System shall support a lifelong identity record, beginning with the assignment of a Unique Identification Number at birth and continuing through updates, suspension, or deactivation in accordance with this Act.
8. The Authority shall establish procedures to enable enrolment through alternative or assisted means for individuals who are unable to provide standard documentation, including through witnesses, community verification, or other lawful methods prescribed by regulations.
9. Regulations may provide for special or differentiated enrolment procedures for categories of persons requiring additional accommodation or verification, including foreign residents, children, and vulnerable individuals.

26. Relationship with civil registration

1. Enrolment in the National Digital Identification System is subject to the primacy of civil registration under section 5 and does not affect civil status.

27. Enrolment procedures

1. Enrolment shall be conducted in accordance with procedures prescribed by regulations, which shall—
   (a) be accessible, transparent, and proportionate;

(b) accommodate assisted, mobile, and offline enrolment modalities; and
(c) include safeguards to prevent fraud while minimising exclusion.

2. The Authority shall ensure that enrolment procedures—
(a) are available without unreasonable fees or charges;
(b) provide clear information to applicants regarding the enrolment process, data collected, and their rights; and
(c) are implemented in a manner consistent with the Data Protection Act.
3. An individual shall not be compelled to enrol in the System as a condition of dignity, existence, or access to emergency or essential public services, except where expressly authorised by written law and subject to safeguards.

(3A) Without prejudice to subsection (3), Parliament may, by written law, require enrolment in the System for specified purposes, sectors, or categories of persons, where such requirement—
(a) is necessary and proportionate to a legitimate public objective;
(b) is accompanied by appropriate safeguards to prevent exclusion or discrimination; and
(c) provides for reasonable alternatives or transitional measures where immediate enrolment is not feasible.]

4. The Authority may establish procedures for the enrolment of Belizean citizens residing outside Belize through diplomatic missions, consular posts, or other authorised overseas enrolment facilities.
5. Upon successful enrolment, the Authority may issue one or more forms of identity credentials associated with the individual's record in the Population Register, including physical credentials, digital credentials, or both, in accordance with this Act and regulations.
6. Digital identity credentials may be issued independently or in association with a physical identity credential, and shall be securely linked to the individual's Unique Identification Number and identity record.
7. Regulations may prescribe—
(a) the processes for issuance, activation, suspension, and revocation of physical and digital credentials;
(b) the methods for linking or associating different forms of credentials;
(c) the technical and security requirements applicable to digital credentials; and
(d) the conditions governing the use and acceptance of such credentials for verification and authentication purposes.

28. Deferred and conditional enrolment

1. Where an applicant is unable to satisfy all enrolment requirements at the time of application, the Authority may permit—
(a) deferred enrolment; or
(b) conditional enrolment subject to subsequent verification,
in accordance with regulations.

2. Deferred or conditional enrolment shall not, of itself—
   (a) result in exclusion from public services where lawful alternatives exist; or
   (b) prejudice the individual's right to complete enrolment at a later time.
3. The Authority shall establish reasonable timeframes, review mechanisms, and assistance measures for individuals subject to deferred or conditional enrolment.

29. Assisted enrolment and special measures

1. The Authority shall implement special measures to facilitate enrolment for—
   (a) persons with disabilities;
   (b) children, older persons, and persons lacking legal capacity;
   (c) persons residing in rural, remote, or underserved areas; and
   (d) any other group at risk of exclusion.
2. Assisted enrolment may include—
   (a) the presence of trained officers or authorised assistants;
   (b) mobile or community-based enrolment services;
   (c) alternative identity verification pathways; and
   (d) reasonable accommodation of physical, sensory, or cognitive impairments.
3. The absence or failure of biometric capture shall not automatically prevent enrolment where alternative lawful identification or assurance mechanisms are available.

30. Non-exclusion and continuity of services

1. No person shall be denied access to a public service solely on the basis that—
   (a) they are not enrolled in the System;
   (b) their enrolment is deferred or conditional; or
   (c) a verification or authentication attempt fails, or they are unable to produce or use an identity credential,
   where lawful alternative means of identification or service delivery exist.
2. Every public authority relying on the System shall maintain fallback procedures to ensure continuity of services in accordance with regulations.
3. The Authority shall periodically assess the impact of enrolment practices on inclusion and shall take corrective measures where systemic exclusion risks are identified.

31. Review and appeal

1. An applicant or affected person who is—
   (a) refused enrolment;
   (b) subjected to deferral, suspension, or deactivation; or
   (c) otherwise materially adversely affected by a decision under this Act,

may apply for administrative review within 30 days of written notification of the decision.

2. Administrative review shall be conducted by a senior officer not involved in the original decision or by a Review Panel appointed by the Board.
3. The reviewing authority shall—
   (a) afford the person a reasonable opportunity to make representations;
   (b) consider all relevant evidence;
   (c) determine whether the decision was lawful, procedurally fair, proportionate, and reasonable; and
   (d) issue a reasoned written determination within 45 days.
4. Where a decision restricts rights or access to services, the burden lies on the Authority to justify its lawfulness and proportionality.
5. A person dissatisfied with the outcome of administrative review may appeal in accordance with section 77.

PART V – IDENTITY DATA AND BIOMETRICS

32. Categories of identity data

1. The Authority may collect and process only such identity data as is **necessary and proportionate** for the purposes of this Act.
2. Identity data under this Act may include—
   (a) **biographic data**, including name, date of birth, sex, and such other attributes as may be prescribed;
   (b) **demographic data**, including address or contact information where required for administrative purposes; and
   (c) **biometric data**, subject to the safeguards and limitations set out in this Part.
3. Identity data shall not include—
   (a) political opinions, religious beliefs, or trade union membership;
   (b) health, genetic, or medical information, except where expressly authorised by written law and not for identification purposes; or
   (c) any category of data prescribed as prohibited by regulations.

32A. Duty to maintain accurate identity data

1. A person enrolled in the National Digital Identification System shall, where reasonably practicable, notify the Authority of any material change to identity data recorded.
2. Material changes may include—
   - (a) change of name;
   - (b) change of address or contact information; or
   - (c) correction of inaccurate identity data.
3. Notification under subsection (1) shall be made in accordance with procedures prescribed by regulations.
4. Failure to notify the Authority under this section shall not, of itself—
   - (a) invalidate the individual's identity record; or

- (b) result in suspension of services.

33. Lawful basis and purpose limitation

1. Identity data, including biometric data, shall be collected, processed, and used **only for purposes expressly authorised under this Act**.
2. Without limiting subsection (1), authorised purposes are limited to—
   (a) enrolment of individuals in the System;
   (b) prevention of duplicate or fraudulent registration through deduplication; and
   (c) verification or authentication of identity claims in accordance with this Act.
3. Identity data shall not be processed for—
   (a) surveillance, monitoring, or tracking of individuals;
   (b) profiling, scoring, or behavioural analysis;
   (c) commercial exploitation or marketing; or
   (d) law enforcement or national security purposes, except where expressly authorised by written law.
4. Identity data collected for one authorised purpose shall not be reused for another purpose unless—
   (a) that subsequent use is expressly authorised by written law; and
   (b) the use is necessary and proportionate to that purpose.

34. Biometric data as a technical tool

1. Biometric data may be used under this Act **solely as a technical means** to—
   (a) establish uniqueness for enrolment and deduplication; or
   (b) authenticate identity claims.
2. **Biometric matching, comparison, or deduplication does not, of itself, constitute legal verification of identity**, status, entitlement, or eligibility.
3. No adverse legal or administrative decision shall be taken solely on the basis of a biometric match, mismatch, or failure, without human review where required.

35. Approved biometric modalities

1. The Authority may approve one or more biometric modalities for use under this Act, subject to this Part and regulations.
2. Approved biometric modalities may include—
   (a) facial images;
   (b) fingerprints; and
   (c) such other modalities as may be approved by the Authority by notice, excluding those prohibited under section 36.
3. In approving a biometric modality, the Authority shall assess—
   (a) accuracy, reliability, and suitability;
   (b) risks of error, exclusion, or discrimination;

(c) privacy and data protection implications; and
(d) availability of reasonable alternatives.

4. Different biometric modalities may be approved for different functions, and the Authority may restrict a modality to specific purposes or contexts.

36. Prohibited biometric modalities and practices

1. The following shall **not** be collected or used for the purposes of this Act—
(a) DNA or genetic data;
(b) behavioural biometrics, including gait, keystroke dynamics, voice patterns, or emotion recognition;
(c) biometric inference of race, ethnicity, health, or other sensitive attributes; or
(d) biometric data derived from covert or non-consensual capture.
2. Biometric data shall not be used—
(a) to train artificial intelligence or machine learning models;
(b) for research, testing, analytics, or system development; or
(c) for any secondary purpose not expressly authorised under this Act.

37. Collection and capture safeguards

1. Biometric data shall be collected only—
(a) by authorised operators;
(b) using approved devices; and
(c) in accordance with technical standards and directions issued by the Authority.
2. The Authority shall ensure that biometric capture procedures—
(a) are transparent and explained to the individual;
(b) include reasonable accommodation for disability or other legitimate limitations; and
(c) permit alternative lawful identification mechanisms where biometric capture is impracticable.
3. No person shall be compelled to submit biometric data where—
(a) it would be unreasonable or disproportionate to do so; or
(b) lawful alternatives are required to be made available under this Act.

38. Security, retention, and lifecycle management

1. Identity and biometric data shall be protected by appropriate technical and organisational measures to ensure confidentiality, integrity, and availability.
2. Biometric data shall—
(a) be encrypted at the point of capture;
(b) be stored separately from biographic data where practicable; and
(c) be retained only for so long as necessary for authorised purposes.
3. The Authority shall establish retention and deletion schedules by regulations, taking into account—
(a) accuracy and integrity requirements;

(b) risks to individual rights; and
(c) applicable data protection obligations.

38A. Privacy-by-design and privacy-enhancing techniques

1. In the design, development, implementation, and operation of the National Digital Identification System, the Authority shall adopt a **privacy-by-design and privacy-by-default approach**.
2. Without limiting subsection (1), the Authority shall, where technically feasible, implement **privacy-enhancing techniques** including—
   (a) pseudonymization;
   (b) tokenization; and
   (c) logical separation of identifiers from biographic and biometric data,
   in order to minimise risks to individuals and prevent unauthorised correlation of identity data.
3. The measures adopted under this section shall ensure that—
   (a) only the minimum data necessary for a lawful and specified purpose is processed; and
   (b) identity data is protected against unauthorised access, linkage, or misuse.
4. The Authority shall periodically review and update the measures adopted under this section to reflect technological developments, emerging risks, and applicable standards.

39. Access restrictions and disclosure

1. Access to identity or biometric data shall be limited to—
   (a) authorised personnel acting within the scope of their duties; and
   (b) authorised systems operating under approved protocols.
2. Biometric data shall not be disclosed to—
   (a) public authorities other than the Authority;
   (b) private entities; or
   (c) foreign governments or international organisations,
   except where expressly authorised by written law and subject to safeguards.
3. The Authority shall implement role-based and purpose-limited access controls ensuring that identity data, including verification responses, are accessible only to authorised persons strictly on a need-to-know basis.
4. No relying party shall obtain visibility into identity data beyond the minimum attributes necessary for the authorised transaction.
5. Any unauthorised access, disclosure, or misuse of biometric data constitutes a serious breach of this Act.

40. Review of biometric necessity and proportionality

1. The Authority shall periodically review—
   (a) the necessity of biometric data collection;

(b) the suitability of approved modalities; and
(c) the risks associated with biometric processing.

2. Where a biometric modality is no longer necessary or proportionate, the Authority shall—
(a) suspend or withdraw its approval; and
(b) take steps to mitigate any resulting impact on individuals.
3. Summaries of such reviews shall be published in accordance with section 23.

PART VI – VERIFICATION AND AUTHENTICATION

41. Provision of verification services

1. The Authority may provide verification services to authorised public authorities and authorised private relying parties in accordance with this Act and regulations.
2. **Verification services** shall be provided through authorized access to the System via secure electronic interfaces and shall be limited to confirming—
(a) whether identity data presented corresponds with a current record in the System; and
(b) the level of assurance associated with that correspondence.
3. For the avoidance of doubt, while the **visual inspection** or **standalone scanning** of a credential may be used for **identity validation** in accordance with prescribed standards, such acts do not constitute a "verification service" under this section as they do not involve real-time interaction with the System.
4. The Authority shall prescribe regulations for **alternative validation procedures** to be used in the event of system unavailability or in geographic areas with limited connectivity, ensuring that access to essential services is not unreasonably denied.
5. Verification services shall not disclose underlying identity or biometric data, except as expressly authorised under this Act.
6. Verification and authentication services shall be implemented through privacy-preserving technical interfaces that—

    (a) disclose no more information than is strictly necessary; and
    (b) do not permit the extraction or reconstruction of identity or biometric data by relying parties.

7. Verification services shall not, of themselves, establish that a person is the legitimate holder of an identity credential, which shall require authentication under section 42.

41A. Forms of identity credentials

1. The Authority may issue or recognise one or more forms of identity credentials, including—

(a) **Physical credentials**, including high-security identity cards;
(b) **Digital credentials**, including mobile-based applications, digital identity wallets, or other cryptographically secured representations of identity;
(c) **Representations of credentials**, such as digital symbols, tokens, or machine-readable codes (QR codes) for the purpose of identification or verification; and
(d) **Technical specifications** or such other secure credentials as may be prescribed to ensure interoperability with international standards.

2. Identity credentials issued under this Act may exist in physical, digital, or combined forms and may be linked to a single identity record in the System.
3. The Authority shall ensure that credential options—
   (a) support offline and assisted use; and
   (b) do not result in exclusion of persons lacking access to digital devices or connectivity.

41B. Responsibility for identity credentials

1. A person to whom an identity credential has been issued shall take reasonable steps to safeguard that credential against loss, theft, unauthorised access, or misuse.
2. Where an individual becomes aware that a credential—

   (a) has been lost or stolen; or

   (b) may have been accessed or used without authorisation,
   the individual shall notify the Authority as soon as reasonably practicable.

3. The Authority shall establish procedures for—

   (a) reporting loss or compromise of credentials;

   (b) suspending or replacing compromised credentials; and

   (c) issuing replacement credentials where necessary.

4. No individual shall incur liability solely by reason of loss or compromise of a credential where the individual has complied with this section.

41C. Suspension or cancellation of identity credentials

1. The Authority may suspend or cancel an identity credential where—

   (a) the credential was issued on the basis of false or fraudulent information;

(b) the credential has been lost, stolen, or compromised;

(c) duplicate credentials have been issued for the same individual; or

(d) cancellation is necessary to protect the integrity or security of the System.

2. Before cancelling a credential under subsection (1), the Authority shall—

(a) notify the affected individual; and

(b) provide an opportunity for review in accordance with section 31.

3. Cancellation of a credential shall not, of itself, terminate the individual's enrolment in the System unless otherwise authorised by this Act.

42. Provision of authentication services

1. The Authority may provide authentication services to authorised relying parties for the purpose of confirming that an individual presenting themselves is the holder of a corresponding identity record.
2. Authentication services shall operate through—
(a) physical or digital identity credentials or factors issued under this Act, including mobile or application-based credentials;
(b) multi-factor or step-up mechanisms where required; or
(c) alternative lawful mechanisms prescribed by regulations.
3. Authentication services shall be designed to minimise data disclosure and shall not require biometric data where a less intrusive method is sufficient.

43. Levels of assurance and proportionality

1. Verification and authentication services shall be provided at **different levels of assurance**, commensurate with—
(a) the purpose of the service;
(b) the risks involved; and
(c) the potential impact on the rights of individuals.
2. No relying party shall require a level of assurance that is disproportionate to the service or transaction concerned.
3. The Authority shall prescribe assurance levels and applicable safeguards by regulations or technical directions.

44. Legal effect and limits of verification and authentication

1. The administrative and non-determinative character of verification and authentication responses is governed by section 7.

2. A relying party shall not—
   (a) treat a verification failure as conclusive proof of ineligibility;
   (b) infer adverse characteristics from a mismatch, non-match, or system unavailability; or
   (c) rely solely on automated responses without human review where an adverse effect may result.
3. Any legal effect attributed to a verification or authentication response must be expressly provided by written law.
4. A valid authentication carried out using a credential issued under this Act shall be recognised as proof of identity for administrative and transactional purposes, subject to applicable law and prescribed levels of assurance.

45. Mandatory fallback and service continuity

1. Every public authority relying on verification or authentication services under this Act shall maintain **lawful fallback procedures** to ensure continuity of services.
2. A person shall not be denied, suspended, or withdrawn from a public service solely because—
   (a) they are unable or unwilling to authenticate through the System;
   (b) a verification or authentication attempt fails; or
   (c) the System is unavailable or experiencing technical issues,
   where lawful alternatives exist.
3. Fallback procedures shall be—
   (a) proportionate to the service concerned;
   (b) accessible to persons at risk of exclusion; and
   (c) periodically reviewed for effectiveness.
4. Where verification or authentication through the System is unavailable or unsuccessful, public authorities and authorised relying parties shall provide reasonable alternative means for establishing identity.

46. Authorisation and obligations of relying parties

1. Only authorised relying parties may access verification or authentication services under this Act.
2. An authorised relying party shall—
   (a) use verification or authentication services only for the purpose authorised;
   (b) comply with assurance levels and safeguards prescribed;
   (c) maintain audit logs of all verification and authentication requests; and
   (d) implement internal procedures to prevent misuse or over-reliance.
3. A relying party shall not store, reuse, or correlate verification or authentication responses beyond what is necessary for the authorised purpose.

46A. Consent for authentication

1. A relying party shall obtain the informed consent of an individual before requesting verification or authentication of that individual through the System, except where—

    (a) such verification is expressly authorised by written law; or

    (b) the request is necessary for the prevention of fraud or misuse of services.

2. Consent under subsection (1) shall—

    (a) be specific to the transaction concerned; and

    (b) be obtained through a clear and transparent process.

3. The Authority shall ensure that authentication interfaces enable individuals to understand—

    (a) the purpose of the authentication request; and

    (b) the identity of the relying party making the request.

4. A relying party shall not store authentication responses or associated metadata except where authorised by law and necessary for the transaction concerned.

47. Logging, transparency, and accountability

1. The Authority shall ensure that all verification and authentication transactions are securely logged for audit and oversight purposes.
2. Logs shall record—
   (a) the identity of the relying party;
   (b) the date, time, and purpose of the request; and
   (c) the type of response provided.
3. Individuals shall have the right, in accordance with the Data Protection Act, to obtain information about verification or authentication requests made in respect of them.

47A. Retention of authentication records

1. The Authority may maintain records of verification and authentication transactions for the purposes of—

    (a) system integrity;

(b) audit and accountability; and

(c) detection and investigation of misuse.

2. Records maintained under this section shall include only the minimum information necessary for those purposes.
3. Authentication transaction records shall not be retained for longer than the period prescribed by regulations, which shall not exceed two years unless required for investigation of a security incident or legal proceeding.
4. Such records shall not be used for profiling, tracking, or behavioural monitoring of individuals.

48. Prohibition of automated adverse decisions

1. No adverse legal or administrative decision affecting an individual shall be based solely on—
   (a) an automated verification or authentication response; or
   (b) a biometric match, mismatch, or system failure.
2. Where a verification or authentication response contributes to a decision with legal or significant effects, the individual shall have—
   (a) the right to human review;
   (b) the opportunity to present additional information; and
   (c) access to review or appeal mechanisms under this Act or other written law.

49. Suspension or restriction of services

1. The Authority may suspend or restrict access to verification or authentication services by a relying party where—
   (a) the relying party breaches this Act or regulations;
   (b) continued access poses a risk to individuals' rights or system integrity; or
   (c) misuse or over-reliance is identified.
2. Any suspension or restriction shall be—
   (a) proportionate;
   (b) subject to review; and
   (c) notified to affected relying parties in writing.

PART VII – AGENCY AND PRIVATE SECTOR RELIANCE

50. Authorisation of relying parties

1. Only a public authority or private entity **authorised under this Act** may rely on verification or authentication services provided by the Authority.
2. Authorisation shall be granted only where the Authority is satisfied that the relying party—
   (a) has a lawful mandate to verify or authenticate identity;

(b) demonstrates necessity and proportionality for the proposed use;
(c) has adequate technical, organisational, and security safeguards in place; and
(d) is capable of complying with this Act, regulations, and applicable data protection obligations under the Data Protection Act.

3. Authorisation may be subject to conditions, limitations, or safeguards prescribed by the Authority.

51. Purpose specification and scope of reliance

1. An authorised relying party may rely on the System **only for the specific purpose** for which authorisation has been granted.
2. A relying party shall not—
(a) expand the scope of reliance beyond the authorised purpose;
(b) use System responses for secondary or unrelated purposes; or
(c) combine System responses with other data to infer characteristics or profiles not authorised by law.
3. Any material change in purpose or scope of reliance requires fresh authorisation.

52. Mandatory non-exclusion impact assessment

1. Before authorising a new use of verification or authentication services by a relying party, the Authority shall require the relying party to conduct a **non-exclusion impact assessment**.
2. A non-exclusion impact assessment shall assess—
(a) risks of exclusion arising from connectivity, documentation gaps, disability, age, or geographic location;
(b) the availability and adequacy of fallback procedures; and
(c) potential disproportionate impacts on vulnerable or marginalised groups.
3. A summary of the assessment and mitigation measures shall be submitted to the Authority and published in such manner as the Authority considers appropriate.

53. Conditions of reliance and safeguards

1. An authorised relying party shall—
(a) rely on System responses only as informational inputs;
(b) implement fallback procedures required under this Act and regulations;
(c) ensure that reliance does not result in automatic adverse outcomes; and
(d) provide clear information to individuals regarding the role of the System in service delivery.
2. Reliance shall be proportionate to the service concerned and shall not require the highest available level of assurance where a lower level is sufficient.

54. Prohibition on data pooling, profiling, and correlation

1. A relying party shall not—
(a) store, pool, or aggregate verification or authentication responses across

services;
(b) use System responses as a general identifier; or
(c) profile, score, rank, or categorise individuals based on System responses.

2. System responses shall not be correlated with other datasets for the purpose of behavioural analysis, eligibility prediction, or social classification.
3. For the purposes of this section, "data pooling" includes the aggregation, combination, or correlation of verification or authentication responses across multiple transactions, services, or datasets for the purpose of profiling, tracking, behavioural analysis, or generating inferences about an individual.
4. Nothing in this section prevents the use of System responses for a specific, lawful, and proportionate purpose authorised under this Act, provided that such use does not involve the creation of persistent profiles, tracking across unrelated services, or unauthorised secondary use of identity data.

55. Logging, audit, and transparency obligations

1. An authorised relying party shall maintain secure logs of all verification and authentication requests, including—
(a) the purpose of the request;
(b) the date and time; and
(c) the outcome of the request.
2. Logs shall be retained only for so long as necessary for audit, accountability, and dispute resolution.
3. Logs shall be made available to—
(a) the Authority;
(b) the Auditor General; and
(c) the Data Protection Commissioner,
for inspection or audit in accordance with law.
4. Any interoperability arrangement shall—
(a) be subject to parliamentary approval;
(b) ensure equivalent or higher standards of data protection; and
(c) include safeguards to prevent misuse, unauthorised access, or onward transfer of identity data.

56. Individual transparency and rights

1. An individual has the right, in accordance with regulations and applicable data protection law, to—
(a) be informed that a relying party has used the System in relation to them;
(b) obtain information about the purpose and outcome of such reliance; and
(c) seek correction, review, or redress where reliance results in adverse effects.
2. Relying parties shall cooperate with the Authority and oversight bodies in responding to individual complaints or reviews.

57. Suspension, revocation, and sanctions

1. The Authority may suspend or revoke a relying party's authorisation where—
   (a) the relying party breaches this Act or regulations;
   (b) reliance practices pose a risk to individual rights or inclusion; or
   (c) the relying party fails to maintain required safeguards.
2. Suspension or revocation shall—
   (a) be proportionate to the breach;
   (b) be subject to review; and
   (c) be notified in writing, with reasons provided.
3. The Authority may impose administrative sanctions in accordance with Part XI.

PART VIII – REGIONAL AND CROSS-BORDER IDENTITY INTEROPERABILITY

58. Purpose of this Part

1. The purpose of this Part is to enable limited, secure, and rights-preserving interoperability of identity credentials issued under this Act for prescribed regional or cross-border purposes.
2. This Part shall be interpreted and applied in a manner that—
   (a) supports lawful mobility, access to services, and regional integration;
   (b) preserves the primacy of this Act and applicable data protection legislation; and
   (c) prevents misuse, over-reach, or function creep in cross-border identity use.

59. Permitted forms of interoperability

1. Interoperability under this Part may take the form of—
   (a) mutual recognition of identity credentials;
   (b) validation of identity attributes presented by an individual; or
   (c) confirmation of the authenticity of a credential,
   without permitting direct access to the Population Register.
2. Interoperability shall not involve—
   (a) interconnection of population registers;
   (b) replication or mirroring of identity databases; or
   (c) continuous or automated cross-border data exchange.

60. Conditions for regional or cross-border recognition

1. No interoperability arrangement under this Part shall be implemented unless—
   (a) the foreign or regional identity system provides safeguards for personal and biometric data that are substantially equivalent to those provided under this Act and applicable data protection legislation;

(b) the purposes of interoperability are specific, limited, and lawful; and
(c) participation by individuals is voluntary and purpose-specific.

2. The Authority shall conduct and publish an assessment addressing—
(a) legal and regulatory equivalence;
(b) technical and security safeguards;
(c) risks of exclusion, discrimination, or misuse; and
(d) availability of remedies and redress.

3. For the purposes of subsection (1)(a), protections shall be considered substantially equivalent only where the foreign or regional identity framework provides, in law and in practice—

(a) independent oversight by a competent supervisory authority;
(b) enforceable data protection rights, including access, correction, and redress;
(c) restrictions on biometric data use comparable to those under this Act;
(d) limits on secondary use and profiling;
(e) effective remedies for unlawful processing; and
(f) safeguards against mass surveillance, tracking, or social scoring.

61. Prohibition on transfer of biometric data

1. Biometric data processed under this Act shall not be transferred, disclosed, or made accessible to—
(a) foreign governments;
(b) regional bodies; or
(c) international organisations,
for the purposes of interoperability under this Part.

2. Nothing in this Part authorises—
(a) export of biometric templates;
(b) remote biometric matching by foreign systems; or
(c) cross-border biometric deduplication.

62. Limits on identity data exchange

1. Any exchange of identity data under this Part shall be limited to—
(a) confirmation responses; or
(b) minimal attribute validation,
strictly necessary for the prescribed purpose.

2. Identity data exchanged under this Part shall not—
(a) be retained beyond the completion of the relevant transaction;
(b) be reused for secondary purposes; or
(c) be combined with other datasets for profiling or surveillance.

3. Identity data exchanged under interoperability arrangements shall be limited to what is necessary, proportionate, and authorised by law and shall not include biometric data except where expressly permitted under this Act.

63. Parliamentary approval of interoperability arrangements

1. No regional or cross-border interoperability arrangement shall take effect unless—
   (a) it is approved by resolution of the National Assembly; and
   (b) the terms of the arrangement are published.
2. An arrangement under this section shall specify—
   (a) participating States or entities;
   (b) purposes and permitted uses;
   (c) categories of data involved;
   (d) safeguards and oversight mechanisms; and
   (e) duration and review periods.
3. Any interoperability arrangement shall ensure equivalent or higher standards of data protection and include safeguards against misuse, unauthorised access, or onward transfer.

64. Voluntary participation and consent

1. An individual shall not be required to rely on interoperability under this Part as a condition of—
   (a) legal status;
   (b) access to essential public services; or
   (c) enjoyment of rights guaranteed under law.
2. Where interoperability is offered, the individual shall be—
   (a) informed of the purpose and scope of the transaction;
   (b) informed of the foreign or regional entity involved; and
   (c) given a meaningful opportunity to consent or decline.

65. Rights to transparency, review, and redress

1. An individual shall have the right to—
   (a) obtain information regarding any cross-border identity verification conducted in respect of them;
   (b) request correction of inaccurate information; and
   (c) seek review or redress where harm arises.
2. The Authority shall ensure that mechanisms for complaint and redress under this Act are accessible in respect of interoperability arrangements.

66. Oversight of interoperability arrangements

1. Interoperability under this Part shall be subject to oversight by—
   (a) the Authority;
   (b) the Auditor General; and
   (c) the Data Protection Commissioner,
   within their respective mandates.

2. Oversight bodies may conduct audits or reviews of—
   (a) technical implementation;
   (b) compliance with safeguards; and
   (c) impacts on individual rights and inclusion.

67. Reporting and periodic review

1. The Authority shall include in its annual report—
   (a) a summary of interoperability arrangements in force;
   (b) purposes and scope of such arrangements;
   (c) any incidents, breaches, or complaints arising; and
   (d) remedial actions taken.
2. Every interoperability arrangement shall be subject to periodic review at intervals not exceeding three years and shall lapse unless renewed in accordance with this Part.

68. Savings and non-derogation

1. Nothing in this Part shall be construed as—
   (a) limiting the rights of individuals under this Act or applicable data protection legislation;
   (b) authorising surveillance, tracking, or monitoring of individuals; or
   (c) permitting use of identity data for law enforcement or national security purposes, except where expressly authorised by written law.
2. In the event of inconsistency between this Part and any interoperability arrangement, this Part shall prevail.

PART IX – RIGHTS OF INDIVIDUALS

69. General principle of individual rights

1. Every individual whose identity data is processed under this Act shall enjoy the rights set out in this Part, in addition to any rights conferred under other written law.
2. The exercise of rights under this Part shall not be made conditional on enrolment status, possession of credentials, or successful authentication.
3. Nothing in this Act shall be interpreted so as to diminish the inherent dignity or legal personhood of any individual.

70. Right to information and transparency

1. An individual has the right to be informed, in clear and accessible language, of—
   (a) the identity of the Authority and any authorised relying party processing their

identity data;
(b) the purposes for which their identity data is processed;
(c) the categories of data collected, including any biometric data;
(d) the consequences of verification or authentication outcomes; and
(e) the rights and remedies available under this Act.

2. Information under subsection (1) shall be provided—
(a) at the time of enrolment; and
(b) upon request, without unreasonable delay or charge.
3. Information shall be provided in accessible formats, including for persons with disabilities and persons with limited literacy.

71. Right of access to identity data

1. An individual has the right to obtain confirmation as to whether identity data relating to them is being processed under this Act.
2. Upon request, the individual is entitled to access—
(a) their biographic and demographic identity data;
(b) information on approved biometric modalities associated with their record;
(c) a summary of verification and authentication requests made in respect of them; and
(d) such other information as may be prescribed.
3. Access shall be provided within a reasonable timeframe prescribed by regulations and at no cost, except where a fee is expressly authorised by written law.

72. Right to correction and rectification

1. An individual has the right to request correction of inaccurate, incomplete, or outdated identity data.
2. The Authority shall—
(a) correct the data without undue delay where the request is substantiated; or
(b) provide written reasons where correction is refused or deferred.
3. Pending correction, the Authority shall take reasonable measures to prevent adverse effects arising from disputed data

73. Right to objection and restriction of processing

1. An individual may object to the processing of their identity data where—
(a) the processing is alleged to be unlawful or disproportionate; or
(b) the processing results in, or is likely to result in, significant harm or exclusion.
2. Upon receipt of an objection, the Authority shall—
(a) assess the objection;
(b) restrict or suspend processing where appropriate; and
(c) notify the individual of the outcome and reasons.
3. The right to object under this section is without prejudice to any rights under the Data Protection Act.

74. Right to human review

1. An individual has the right to request **human review** of—
   (a) any adverse decision or outcome materially influenced by a verification or authentication response; or
   (b) any refusal, suspension, or restriction of enrolment or access under this Act.
2. Human review shall—
   (a) be conducted by a competent and authorised officer;
   (b) take into account information provided by the individual; and
   (c) not be based solely on automated or technical processes.
3. The outcome of a human review shall be communicated in writing, with reasons provided.

75. Right to access verification and authentication logs

1. An individual has the right to obtain information regarding—
   (a) the identity of authorised relying parties that have made verification or authentication requests in respect of them;
   (b) the purposes for which such requests were made; and
   (c) the dates and outcomes of such requests.
2. Access to logs may be subject to reasonable limitations prescribed by regulations to protect—
   (a) system security; or
   (b) the rights of third parties.

76. Right to complaint and redress

1. An individual may lodge a complaint with—
   (a) the Authority;
   (b) an oversight body; or
   (c) any other body prescribed by law,
   where they allege a breach of this Act or harm arising from reliance on the System.
2. Complaints shall be—
   (a) acknowledged promptly;
   (b) investigated impartially; and
   (c) resolved within reasonable timeframes prescribed by regulations.
3. The complainant shall be informed of the outcome and any remedial measures taken.

77. Right to appeal and judicial remedies

1. A person aggrieved by—
   (a) a decision of the Authority following administrative review;
   (b) the imposition of an administrative sanction;
   (c) suspension or revocation of authorisation; or

(d) issuance of a binding direction,

may appeal to an independent tribunal established under written law or prescribed by regulations.

2. The tribunal shall be independent of the Authority and may review questions of fact and law.
3. The tribunal may affirm, vary, set aside, or substitute the decision and may grant interim relief where justice so requires.
4. Nothing in this Act limits the right of a person to seek judicial review, constitutional relief, or any other remedy available under law.

78. Assistance and representation

1. The Authority shall ensure that individuals—
   (a) are informed of their rights under this Part; and
   (b) have access to reasonable assistance in exercising those rights.
2. An individual may be assisted or represented by another person of their choosing, including a legal representative, advocate, or authorised assistant.

PART X – OVERSIGHT, AUDIT, AND ACCOUNTABILITY

79. Principle of independent and concurrent oversight

1. Oversight of the System and all processing of identity data under this Act shall be exercised through **independent and concurrent oversight mechanisms**.
2. No single authority, including the National Identification Authority, shall have exclusive or final oversight responsibility under this Act.
3. Oversight shall be exercised in a manner that—
   (a) protects individual rights and dignity;
   (b) ensures accountability and transparency; and
   (c) prevents misuse, abuse, or function creep.

80. Oversight bodies

1. Oversight of this Act shall be exercised by—
   (a) the National Identification Authority, in respect of operational compliance;
   (b) the Auditor General, in respect of financial, performance, and systems audits; and
   (c) the Data Protection Commissioner, in respect of personal and biometric data protection.
2. Each oversight body shall exercise its functions **independently** and in accordance with its enabling legislation.
3. Nothing in this Act limits the powers of an oversight body under any other written law.

81. Audit and inspection powers

1. An oversight body may, for the purposes of this Act—
   (a) conduct audits or inspections of the Authority, authorised operators, and relying parties;
   (b) require the production of records, logs, technical documentation, and audit trails;
   (c) enter premises at reasonable times, subject to law; and
   (d) make findings, recommendations, or directives within its lawful mandate.
2. Audit access under this Act shall not be limited by—
   (a) confidentiality claims;
   (b) technical or proprietary arrangements; or
   (c) contractual terms,
   except where expressly provided by written law.
3. A person who obstructs or fails to cooperate with an audit or inspection commits an offence under this Act.

82. Triggered and special audits

1. In addition to routine audits, an oversight body may conduct a **triggered audit** where—
   (a) a significant incident or breach occurs;
   (b) systemic exclusion or discrimination is alleged;
   (c) credible misuse or over-reliance is identified; or
   (d) directed by Parliament.
2. Triggered audits may include—
   (a) technical system audits;
   (b) algorithmic or biometric performance audits;
   (c) inclusion and non-exclusion impact audits; or
   (d) compliance audits of relying parties.

83. Reporting and publication

1. The Authority shall submit an annual report to Parliament in accordance with section 23, which shall include—
   (a) summaries of audits conducted;
   (b) incidents and breaches reported;
   (c) corrective measures taken; and
   (d) identified risks or systemic issues.
2. Oversight bodies may publish audit summaries, findings, or recommendations, subject to lawful confidentiality limitations.
3. Reports shall be published in a manner that promotes public understanding and accountability.

84. Parliamentary oversight

1. The Minister shall table the annual report of the Authority in the National Assembly within a prescribed period.
2. Parliament may—
   (a) refer any report or audit finding to a committee;
   (b) require the appearance of the Authority or any oversight body; or
   (c) make recommendations for legislative or policy action.

85. Corrective measures and binding directions

1. Where an oversight body acting within its lawful mandate identifies non-compliance or systemic risk, it may—
   (a) issue recommendations;
   (b) require corrective measures within a specified timeframe, where authorised under written law; or
   (c) refer the matter for enforcement action.
2. Binding directions issued under this section shall—
   (a) be proportionate;
   (b) be reasoned and documented; and
   (c) respect due process.
3. A person subject to a binding direction under this section shall have the right to seek administrative review and appeal in accordance with sections 31 and 66.
4. Corrective measures required under this section shall be binding where issued pursuant to statutory powers under applicable law.

86. Whistleblower protection

1. A person who, in good faith, discloses information relating to—
   (a) misuse of the System;
   (b) unlawful processing of identity or biometric data; or
   (c) systemic risks or failures,
   shall not be subject to civil, criminal, or disciplinary liability for making such disclosure.
2. Retaliation against a whistleblower is prohibited and constitutes an offence.

87. Review of oversight framework

1. The Minister shall cause a review of the oversight framework established under this Act to be conducted—
   (a) within three years of commencement; and
   (b) at such intervals thereafter as may be prescribed.
2. The review shall assess—
   (a) effectiveness of oversight mechanisms;
   (b) adequacy of safeguards; and
   (c) emerging risks or gaps.

3. A report of the review shall be laid before Parliament.

PART XI – SECURITY AND INCIDENT RESPONSE

88. Duty to ensure security of identity data

1. The Authority shall ensure that appropriate **technical and organisational measures** are implemented to protect identity data processed under this Act against—
   (a) unauthorised or unlawful access, disclosure, alteration, or destruction;
   (b) accidental loss or damage; and
   (c) threats to confidentiality, integrity, or availability.
2. Security measures shall be—
   (a) proportionate to the sensitivity of the data, including biometric data;
   (b) regularly reviewed and updated; and
   (c) consistent with standards and directions issued under this Act.
3. Security obligations under this section apply equally to—
   (a) the Authority;
   (b) authorised biometric operators; and
   (c) authorised relying parties, within the scope of their access.

89. Risk management and security governance

1. The Authority shall establish and maintain a **risk management framework** addressing—
   (a) technical vulnerabilities;
   (b) operational and human risks;
   (c) supply chain and vendor risks; and
   (d) risks of exclusion, misuse, or abuse.
2. The risk management framework shall include—
   (a) periodic risk assessments;
   (b) security testing and evaluation;
   (c) access control and credential management; and
   (d) segregation of duties and least-privilege principles.
3. Summaries of risk assessments may be included in reports published under this Act, subject to lawful security limitations.

90. Incident detection and internal response

1. The Authority and all authorised operators shall implement procedures to—
   (a) detect actual or suspected incidents affecting identity or biometric data;
   (b) assess the nature, scope, and impact of such incidents; and
   (c) take immediate steps to contain and mitigate harm.
2. Incident response procedures shall ensure—
   (a) prompt internal escalation;

(b) preservation of evidence; and
(c) documentation of actions taken.

3. No person shall conceal, delay, or misrepresent an incident required to be addressed under this Act.

91. Mandatory incident notification to the Authority

1. An authorised operator or relying party shall notify the Authority **without undue delay** upon becoming aware of—
(a) an actual or suspected compromise of identity or biometric data; or
(b) any incident that materially affects the security, integrity, or availability of the System.
2. Notification under subsection (1) shall include—
(a) a description of the incident;
(b) the categories of data affected;
(c) known or suspected impacts; and
(d) measures taken or proposed to address the incident.
3. Failure to notify the Authority as required constitutes a breach of this Act.

92. Authority response and remedial powers

1. Upon receiving notification of an incident, the Authority may—
(a) require specified remedial or corrective actions;
(b) conduct or direct an investigation;
(c) impose temporary safeguards, restrictions, or suspensions; or
(d) refer the matter to an oversight body or enforcement authority.
2. Measures taken under subsection (1) shall be—
(a) proportionate to the severity of the incident; and
(b) directed at preventing recurrence and mitigating harm.

93. Notification to affected individuals

1. Where an incident involving identity or biometric data is likely to result in a high risk to the rights or interests of individuals, the Authority shall ensure that affected individuals are notified without undue delay, and in any event within 60 days, and may direct the relevant authorised operator or relying party to effect such notification on its behalf.
2. Notification under subsection (1) shall include—
(a) the nature of the incident;
(b) the categories of data affected;
(c) measures taken or proposed to mitigate harm; and
(d) recommended steps individuals may take to protect themselves.
3. The Authority may direct—
(a) the timing;
(b) the form; and

(c) the manner of notification,
having regard to the risk, urgency, and practical circumstances.

4. This section is without prejudice to notification obligations under the Data Protection Act.

94. Incident classification and record-keeping

1. The Authority shall maintain a register of incidents, including—
   (a) the nature and severity of incidents;
   (b) remedial actions taken; and
   (c) outcomes of investigations or audits.
2. Incident records shall be retained for audit, oversight, and accountability purposes.
3. Non-sensitive summaries of incidents may be included in reports published under this Act.

95. Coordination with oversight and security bodies

1. The Authority shall cooperate with—
   (a) oversight bodies referred to in Part IX; and
   (b) any national cybersecurity or public safety bodies prescribed by law,
   in responding to incidents.
2. Cooperation under subsection (1) shall not—
   (a) expand the purposes for which identity data may be used; or
   (b) permit disclosure of biometric data except as authorised by written law.

96. Testing, preparedness, and continuous improvement

1. The Authority shall ensure that incident response procedures are—
   (a) tested periodically;
   (b) reviewed following significant incidents; and
   (c) updated to reflect evolving risks and best practice.
2. Lessons learned from incidents shall inform—
   (a) system design improvements;
   (b) training and awareness; and
   (c) revisions to standards or directions issued under this Act.

PART XII – OFFENCES AND ENFORCEMENT

97. General principles governing enforcement

1. Enforcement under this Act shall be guided by the principles of—
   (a) legality and due process;
   (b) proportionality;

(c) accountability for abuse of authority; and
(d) protection of individuals from harm or exclusion.

2. No person shall be subjected to criminal liability under this Act solely for—
(a) failure to enrol in the System;
(b) inability to authenticate or verify identity; or
(c) reliance on alternative lawful identification methods.
3. A contravention of any prohibition under this Act may give rise to criminal liability, administrative sanction, or civil remedy as provided under this Part and Part XI.

98. Unauthorised access and misuse of identity data

1. A person commits an offence if that person—
(a) knowingly accesses identity or biometric data without authorisation;
(b) knowingly discloses such data to an unauthorised person; or
(c) knowingly uses such data for a purpose not authorised under this Act.
2. A person guilty of an offence under this section is liable on conviction—
(a) on summary conviction, to a fine not exceeding an amount prescribed by regulations or to imprisonment for a term not exceeding two years, or to both;
(b) on conviction on indictment, to a fine or to imprisonment for a term not exceeding five years, or to both.

99. General penalty provision

Where an act or omission constitutes an offence under this Act and no specific penalty is provided, the person is liable—
(a) on summary conviction, to a fine not exceeding the amount prescribed under section 87(2)(a) or to imprisonment for a term not exceeding two years, or to both;
(b) on conviction on indictment, to a fine or imprisonment not exceeding five years, or to both.

Nothing in this section limits the imposition of administrative sanctions under Part XI.

100. Abuse of authority or position

1. A public officer, employee of the Authority, or authorised operator commits an offence if that person—
(a) uses their position to improperly access or influence the System;
(b) authorises or facilitates unlawful reliance or data processing; or
(c) acts in a manner intended to cause harm, exclusion, or discrimination.
2. An offence under this section shall be treated as an aggravating offence for sentencing purposes.

101. Obstruction of oversight and audit

1. A person commits an offence if that person—
   (a) obstructs or interferes with an audit or inspection under this Act;
   (b) knowingly provides false or misleading information to an oversight body; or
   (c) destroys, conceals, or alters records relevant to oversight.
2. A person convicted under this section is liable to penalties prescribed under section 87.

102. Failure to comply with binding directions

1. A person or entity commits an offence if they—
   (a) fail, without reasonable excuse, to comply with a binding direction lawfully issued under this Act; or
   (b) continue unauthorised reliance or processing after suspension or revocation.
2. In determining liability, the court shall consider—
   (a) the seriousness of the breach;
   (b) whether harm or risk of harm occurred; and
   (c) whether corrective measures were attempted.

103. Corporate liability

1. Where an offence under this Act is committed by a body corporate, the body corporate commits the offence.
2. A body corporate is liable for acts or omissions of its directors, officers, employees, or agents acting within the scope of their authority or employment.
3. A director, manager, secretary, or similar officer also commits the offence if—
   (a) the offence was committed with their consent or connivance; or
   (b) the offence is attributable to their neglect.
4. It shall be a defence for a body corporate to prove that it exercised all reasonable due diligence to prevent the commission of the offence, including the implementation of appropriate compliance, training, and supervisory measures.

104. Administrative sanctions

1. Without prejudice to criminal liability, the Authority may impose **administrative sanctions** for contraventions of this Act or regulations, including—
   (a) warnings or reprimands;
   (b) compliance orders;
   (c) suspension or revocation of authorisation;
   (d) administrative fines, as prescribed.
2. Administrative sanctions shall be—
   (a) proportionate to the breach;
   (b) reasoned and documented; and
   (c) subject to review or appeal.

3. No administrative sanction shall be imposed unless—
   (a) the affected person has been given written notice of the alleged contravention;
   (b) the person has been afforded a reasonable opportunity to respond; and
   (c) the Authority has considered whether the sanction is proportionate to the breach.

105. Civil remedies

1. Nothing in this Act limits the right of any person to seek—
   (a) compensation for loss or damage suffered as a result of a breach of this Act;
   (b) injunctive or declaratory relief; or
   (c) any other civil remedy available under written law.
2. Civil remedies may be sought independently of, or in addition to, enforcement action under this Act or applicable data protection legislation.

106. Protection against retaliation

1. No person shall be subjected to retaliation, penalty, or adverse treatment for—
   (a) exercising rights under this Act;
   (b) making a complaint or request for review; or
   (c) cooperating with an investigation or audit.
2. Retaliation in contravention of this section constitutes an offence.

107. Limitation on liability for good faith actions

1. No civil or criminal liability shall attach to the Authority, an authorised operator, or a public officer for an act done in good faith in the lawful exercise of powers under this Act.
2. Subsection (1) does not apply to—
   (a) gross negligence;
   (b) wilful misconduct; or
   (c) abuse of authority.

PART XIII – MISCELLANEOUS AND TRANSITIONAL

108. Power to make regulations

1. The Minister may, after consultation with the Authority, make regulations for carrying out or giving effect to this Act.
2. Without limiting subsection (1), regulations may provide for—
   (a) enrolment procedures and evidentiary requirements;
   (b) verification and authentication processes;
   (c) assurance levels and fallback mechanisms;
   (d) retention and deletion schedules;
   (e) fees, charges, or exemptions relating to enrolment and the issuance, renewal,

or replacement of identity credentials;
(f) validity periods and renewal requirements for identity credentials;
(g) procedures for the replacement, suspension, or reissuance of identity credentials in cases of loss, theft, or damage;
(h) review, appeal, and complaint procedures; and
(i) any matter required or permitted to be prescribed under this Act.

3. Regulations made under this section shall be consistent with—
(a) the objects and guiding principles set out in Part I; and
(b) the rights and safeguards provided under this Act, including the principles of necessity, proportionality, and data minimisation.

109. Technical directions and standards

1. The Authority may issue **technical directions, standards, and codes of practice** for the implementation of this Act.
2. Technical directions issued under this section may address—
(a) system architecture and interoperability;
(b) biometric capture and processing standards;
(c) security and encryption requirements;
(d) audit logging and reporting formats; and
(e) operational procedures.
3. Technical directions—
(a) shall not expand the purposes for which identity or biometric data may be processed;
(b) shall not diminish rights or safeguards provided under this Act; and
(c) shall be published in a manner accessible to the public, except where limited by lawful security considerations.

110. Parliamentary control over delegated powers

1. Regulations made under this Act shall be subject to **negative resolution** of the National Assembly, unless otherwise provided by written law.
2. The Minister shall ensure that any regulation or technical framework that materially affects individual rights, enrolment obligations, or reliance by public authorities is accompanied by—
(a) an explanatory statement; and
(b) a summary of consultations undertaken.

111. Transitional arrangements

1. The Minister may, by regulations, provide for transitional arrangements to facilitate the implementation of this Act.
2. Transitional arrangements may include—
(a) migration or reconciliation of data from existing identity systems;

(b) phased enrolment or system rollout;
(c) temporary recognition of existing credentials; and
(d) continuity of services during transition.

3. Transitional measures—
(a) shall be time-limited;
(b) shall not lower applicable security or rights safeguards; and
(c) shall not be used to expand the purposes of the System beyond this Act.

4. (1) The regulations listed in Schedule 1 shall, upon the commencement of this Act, be deemed to have been made under this Act to the extent that they are consistent with this Act.

5. (2) The Minister may, by Order published in the Gazette, amend Schedule 1 to reflect the revision, consolidation, or replacement of any regulation listed therein.

112. Savings

1. Nothing in this Act affects—
(a) the operation of the Civil Registry and Vital Statistics Act, 2025;
(b) rights and obligations under the Data Protection Act; or
(c) any lawful act done prior to the commencement of this Act.

2. Any reference in another written law to an identity document or identifier shall not be construed as a reference to the System unless expressly provided.

113. Consequential and incidental matters

1. The Minister may, by regulations, make such incidental or consequential provisions as are necessary to give full effect to this Act.

2. No consequential provision shall—
(a) create new categories of mandatory enrolment;
(b) authorise new biometric modalities; or
(c) limit individual rights,
except by Act of Parliament.

114. Statutory review of the Act

1. The Minister shall cause a review of the operation of this Act to be conducted—
(a) within five years of its commencement; and
(b) at such intervals thereafter as Parliament may determine.

2. The review shall assess—
(a) effectiveness of the System;
(b) impacts on inclusion and access to services;
(c) adequacy of safeguards and oversight; and
(d) emerging technological or societal risks.

3. A report of the review shall be laid before the National Assembly.

SCHEDULE 1 – EXISTING REGULATIONS

1. Citizen Enrolment Regulations, 2026
2. Biometric Data Collection and Management Standards Regulations, 2026
3. Data Verification Regulations, 2026
4. Agency Interaction Regulations, 2026
5. Card Issuance Regulations, 2026
6. Use of NID System for Services Regulations, 2026