Liberty Fighters Network

Est. 2016 - A voluntary association without gain (*Universitas*)

***Office of the President*: Reyno De Beer**

Cellular: +27(0)67 735 7288

Electronic Mail: reyno@libertyfighters.org

Website: www.libertyfighters.org / Telegram: @libertyfightersnews / Twitter: @LFN_SouthAfrica /

Facebook: Libertyfightersnetwork / YouTube: @LibertyFighters

Date: 25 May 2026

FORMAL HOLISTIC COMMENT AND OBJECTION

Draft Amendments to the Identification Regulations, 1998, read with the Identification Regulations, 1998 as currently in force

[*Government Gazette No. 54610, Government Notice R. 7428, dated 4 May 2026*]

To: Chief Director: Legal Services, Department of Home Affairs

Marked for the attention of: Adv A M Malakate

E-mail: Moses.Malakate@dha.gov.za

Submitted by: Liberty Fighters Network, a voluntary association without gain, represented by its President, Reyno De Beer

Contents

1. Executive Summary 3

2. Documents and Approach Considered 5

3. LFN's Core Position 6

4. Constitutional and Statutory Framework 8

5. Holistic Comment on the Current Regulations as They Would Stand After Amendment 10

6. Structural Defects in the Draft Amendment Scheme 16

6.1. Excessive Reliance on Future Instructions 16

6.2. Current Regulation 15(d) May Bypass the New Framework 16

6.3. Ambiguous Use of "Person" Creates Human-Identity and Non-Human Entity Risks 17

6.4. Private-Sector Enrolment Converts Commercial Institutions into Proxy State Agents 19

6.5. Technical and Drafting Errors Must Be Corrected 20

7. Specific Objections and Requested Amendments 21

7.1. Objection 1: Digital IDs Must Never Become Mandatory in Law or Practice 21

7.2. Objection 2: Physical IDs Must Remain Equal and Permanent 21

7.3. Objection 3: Biometrics of Physical-ID Users Must Be Segregated from Digital-ID Infrastructure 22

7.4. Objection 4: Consent Must Be Specific, Informed, Recorded and Transaction-Based 22

7.5. Objection 5: Trusted Entities and Verified Relationships Are Too Broad 23

7.6. Objection 6: Identity Assurance Levels Must Not Create a Two-Tier Citizenry 24

7.7. Objection 7: No Racial, BBBEE or Sensitive Classification 24

7.8. Objection 8: "Person" Must Be Limited to a Natural Living Human Being Where Human Identity Is Concerned 25

7.9. Objection 9: Suspension and Revocation Require Strong Redress 26

7.10. Objection 10: Public Participation Is Inadequate 27

7.11. Objection 11: Operational Readiness and Cybersecurity Must Be Proven 28

7.12. Objection 12: Function Creep Must Be Expressly Prohibited 28

8. Consolidated Proposed Clauses 29

9. Requests 34

10. Conclusion 36

1. Executive Summary

1.1. Liberty Fighters Network ("LFN") submits this holistic comment after considering not only the draft amendments published in *Government Gazette No. 54610* on 4 May 2026, but also the *Identification Regulations, 1998*, as they currently stand. LFN respectfully submits that a proper comment on the draft amendments cannot be limited to the newly proposed digital-identity provisions in isolation. The draft amendments alter the operation, purpose and risk-profile of the entire regulatory scheme.

1.2. LFN does not object to digital identity technology *per se* – for all practical purposes, whether we like it or not, the ship has already left the port and reached its destination over influx of time. Resultantly, a Digital ID may benefit society if it is voluntary, secure, decentralised where possible, rights-compliant, non-discriminatory, and genuinely offered as a convenience. It may assist with fraud prevention, lost documents, emergency identification, service delivery and quicker verification. Those advantages, however, cannot justify compulsory digital identity, centralised biometric exposure, private-sector enrolment, race-based classification, open-ended data sharing, ambiguity around who or what may be identified as a "person", or a system that turns citizenship into a permission-based digital status.

1.3. LFN's position remains that Digital IDs may only exist as an additional option alongside physical identity books/cards, with equal legal effect and equal practical acceptance. No individual may be penalised, delayed, charged more, treated as lower trust, excluded from services, or subjected to inferior administrative treatment because that individual chooses to use a physical ID book/card instead of a Digital ID, or *vice versa*.

1.4. The current Identification Regulations already contain important features which the draft amendments do not adequately reconcile. These include the existing rules on identity numbers, photographs, fingerprints, address changes, physical identity-card applications, duplicates, temporary identity certificates, offences, and fees for furnishing population-register information. In particular, regulation 15(d), as currently amended, already contemplates real-time and batch furnishing of population-register information to any person, organisation, body, society or institution for a fee. This older fee-based data-access mechanism must be expressly subordinated to the new privacy, trusted-entity and consent safeguards, otherwise the new Digital ID safeguards may be bypassed through the existing fee provision.

1.5. LFN further submits that the repeated use of the word "person" in the current and proposed Regulations is a material drafting concern. In South African law, including the *Interpretation Act, 1957*, "*person*" may include juristic persons, bodies corporate, unincorporated bodies and other *personae fictae*. In a modern digital environment, it may also invite unnecessary future arguments concerning artificial intelligence systems, software modules, robots, digital agents, machine identities, corporate profiles, accounts, devices or other non-human entities. A Digital ID framework dealing with biometrics, liveness detection, facial recognition, fingerprints, dignity, privacy, bodily integrity and civic status must be drafted *ex abundanti cautela* to apply only to natural living human beings, unless a provision expressly deals with juristic or institutional entities such as trusted entities.

1.6. The draft amendments contain some welcome wording. Regulation 16(4) states that a Digital ID has the same legal effect as a physical identity card. Regulation 16(5) states that the issuance of a Digital ID does not affect the validity of a physical identity card and that the holder may use either form of identity card. Regulation 18(1) states that a person may, but is not required to, apply for a Digital ID. Regulation 49(3) states that no person is compelled to obtain a Digital ID in order to continue using a valid physical identity card. LFN welcomes these clauses in principle, but they are incomplete because they do not expressly bind private actors, organs of state, accredited trusted entities, banks, mobile operators, insurers, employers, municipalities, educational institutions, healthcare providers, landlords, security providers, or any other person or entity who may in practice refuse physical IDs and thereby make Digital IDs mandatory *de facto*.

1.7. LFN accordingly requests that the draft amendments be withdrawn, alternatively materially amended and republished for a further public-comment process, after publication of all relevant impact assessments, draft instructions, draft data-sharing agreements, cybersecurity certifications, operational-readiness evidence and plain-language summaries in all written official languages, together with accessible formats for persons with disabilities.

2. Documents and Approach Considered

2.1. LFN considered the following documents for purposes of this revised submission:

- *Identification Regulations, 1998*, as currently in force as at 25 May 2026.
- Draft amendments to the Identification Regulations, 1998, published in *Government Gazette No. 54610, Government Notice R. 7428, dated 4 May 2026*.

- LFN's Discussion Paper, "To Digital ID, or Not to Go Digital, That is the Question", November 2025, Version 1.0.

- Civil-society concerns raised by allied voices, insofar as those concerns are relevant to freedom, privacy, equality, lawful administration and protection against direct or indirect compulsion.

- The *Constitution*, the *Identification Act*, the *Interpretation Act*, *POPIA*, *PAJA*, *PAIA*, the *Consumer Protection Act*, *FICA*, and publicly available official material concerning prior authorisation, public participation, identity systems and accessibility.

2.2. This submission is LFN's own independent position. LFN notes aligned civil-society concerns, but does not copy, compare itself with, or purport to adopt any other organisation's objection. The common concern is the preservation of freedom and privacy in a proposed national biometric identity framework.

2.3. LFN has now approached the Regulations holistically. The question is not only whether each new digital provision sounds acceptable in isolation. The proper question is how the current physical-ID framework, the existing population-register access rules, the proposed Digital ID provisions, the trusted-entity model, the Director-General's proposed instruction-making powers, and the repeated use of the word "*person*" will operate together after amendment.

3. LFN's Core Position

3.1. Digital IDs can be an advantage to society, but must never become mandatory, whether expressly, indirectly, commercially, administratively or technologically.

3.2. Digital IDs must permanently co-exist with physical ID books/cards. Both systems must be lawful, functional, equally accepted and non-discriminatory. No individual may be disadvantaged for choosing one system over the other.

3.3. Persons who choose to remain within the physical-ID system must not have their biometric information exposed to, queried through, migrated into, or made available on the systems utilised for Digital IDs, save where expressly authorised by an Act of Parliament, a warrant, or a court order that meets constitutional standards.

3.4. The exchange of personal information between the State and private entities may not occur without clear, informed, specific, recorded and transaction-specific consent by the individual concerned, save for narrow criminal reporting or other statutory duties prescribed by valid legislation.

3.5. Private institutions, including banks, mobile operators, insurers and large retailers, may not be used by the State as collectors, processors, validators or custodians of private information for Digital ID enrolment, biometric capture, identity-assurance scoring, or population-register updating.

3.6. Digital IDs may not store, display, encode, infer, transmit or facilitate access to race, ethnic origin, colour, BBBEE classification, employment-equity classification, health status, vaccination status, political persuasion, religion, trade union membership, or comparable sensitive classifications.

3.7. The regulatory framework must prevent function creep. A Digital ID built for identity verification must not later become a tool for e-voting, social-credit scoring, protest monitoring, medical-status enforcement, political profiling, automated fines, debt collection, commercial analytics, or generalised surveillance.

3.8. The regulatory framework must expressly distinguish between a natural living human being and a juristic, artificial, automated, digital or machine-based entity. Human identity infrastructure must not be capable of being misused or reinterpreted to create identity credentials for personae fictae, artificial intelligence systems, robots, software modules, digital agents, devices, accounts, wallets, corporate profiles, machine identities or other non-human constructs.

4. Constitutional and Statutory Framework

4.1. The draft amendments must comply with the *Constitution of the Republic of South Africa, 1996*. Sections 7(2), 9, 10, 14, 33, 36, 195 and 237 are of direct relevance. Section 7(2) requires the State to respect, protect, promote and fulfil the rights in the Bill of Rights. Section 9 protects equality. Section 10 protects dignity. Section 14 protects privacy. Section 33 protects lawful, reasonable and procedurally fair administrative action. Section 36 controls any limitation of rights. Section 195 demands accountable, transparent and efficient public administration. Section 237 requires constitutional obligations to be performed diligently and without delay.

4.2. The *Identification Act, 1997 (Act No. 68 of 1997)* provides for the compilation and maintenance of the population register and the issuing of identity cards and certificates. Section 7 of the Act provides that an identity number consists only of figure-coded date of birth, gender and citizenship, together with serial, index and control numbers. It does not authorise race to be encoded in the identity number. LFN insists that this position must not be altered, inferred around, or recreated digitally through Digital ID metadata, APIs, assurance levels or machine-readable expressions.

4.3. The *Interpretation Act* is directly relevant to the drafting concern raised herein. The word "*person*" is not inherently limited to a natural living human being. It may include a juristic

person, company, body corporate, unincorporated association or other *persona ficta*. This broad meaning may be suitable in many statutes, but it is dangerous in a biometric Digital ID framework unless the Regulations expressly state when “person” means a natural living human being and when it means an entity or institution.

4.4. *POPIA* is directly implicated. Biometric information is special personal information. Identity numbers and similar identifiers are unique identifiers. Prior-authorisation considerations under sections 57 and 58 of *POPIA* arise where unique identifiers are processed for a purpose other than that for which they were originally collected and with the aim of linking information with information processed by other responsible parties.

4.5. *PAJA* is implicated because the regulations and their implementation materially affect members of the public. Where administrative action materially and adversely affects the rights of the public, section 4 of *PAJA* requires a procedurally fair process appropriate to the magnitude and impact of the decision. A short written-comment period is insufficient for a national biometric identity architecture unless it is accompanied by proper publication, explanation, impact assessment, accessibility measures and meaningful engagement.

4.6. *PAIA* is relevant because the public must be able to request records concerning system design, data-sharing agreements, accredited entities, security audits, uptime, breaches, vendors, tenders, costs, and operational-readiness decisions.

4.7. The *Consumer Protection Act* is relevant because private actors must not deprive consumers of choice or impose unfair, unreasonable or unjust conditions by insisting on Digital ID only, where physical IDs remain legally valid.

4.8. *FICA* and related laws may require accountable institutions to verify identity and report suspicious transactions. That statutory duty must not be converted into a general permission for banks to enrol citizens into Digital ID systems, collect biometrics for the State, or maintain standing population-register data pipes.

5. Holistic Comment on the Current Regulations as They Would Stand After Amendment

5.1. LFN comments on the current Regulations and the proposed amendments together, because the amended regulatory scheme would operate as one integrated instrument. The following table identifies key provisions, the practical concern, and LFN's requested approach.

Provision	Holistic concern	LFN comment / requested amendment
Regulation 1: Definitions and interpretation	The draft substitutes the entire definition regulation and gives new meaning to "trusted entity", "mandatory particulars", "data sharing agreement", "biometric data", "digital identity credential" and "verified relationship". It still uses "person" repeatedly without a sufficient distinction between natural human beings and juristic or artificial entities.	The definitions are too enabling and insufficiently precise. "Mandatory particulars" may be determined by instruction, which allows core identity-content questions to be decided administratively after public comment has closed. Define mandatory particulars exhaustively in the Regulations and expressly exclude race, BBBEE, health, vaccination, political and comparable sensitive classifications. Insert a definition of "individual" or "natural living human being" and use it wherever biometrics, Digital ID credentials, identity cards, liveness detection, identity assurance or population-register particulars are concerned.

Provision	Holistic concern	LFN comment / requested amendment
Regulation 1A: Objects	The draft objects include the population register as an authoritative source and establish physical and digital identity cards as alternative forms.	Insert additional objects: to preserve permanent, equal and non-discriminatory access to physical identity documents and non-digital identity verification for all individuals; and to ensure that human identity infrastructure applies only to natural living human beings, not to juristic, artificial, automated, digital or machine-based entities.
Regulation 1B: Application	The draft separates regulations 4 to 15 for physical identity cards and regulations 16 to 46 for digital credentials and associated arrangements.	The split is artificial because data sharing, verification, fees and population-register access affect both physical and digital users. Insert a supremacy clause that privacy, consent, non-discrimination, human-identity clarity and fallback protections apply across the entire regulatory scheme.
Regulation 2: Population register	The population register remains the central authoritative record.	The register may remain authoritative for civil-status particulars of natural living human beings, but authority does not mean unrestricted digital interconnection. Access must remain tightly controlled, logged,

Provision	Holistic concern	LFN comment / requested amendment
		minimised and consent-based where private entities are involved. The register must not become a registry for AI modules, robots, machine identities, corporate profiles or other non-human entities.
Regulation 3: Identity number	The current identity number encodes date of birth, gender and citizenship, plus serial, index and control numbers. It does not encode race.	LFN supports that race is not encoded and requests express confirmation that no racial, BBBEE or employment-equity classification may be encoded, inferred, generated or linked to the Digital ID or identity number.
Regulations 4 and 8: Photographs and fingerprint on physical identity card	The current physical system already uses photographs and a thumbprint for identity cards.	Existing physical-ID biometrics must not become a gateway into facial-recognition APIs, liveness detection, private-vendor matching or trusted-entity Digital ID verification for individuals who do not voluntarily obtain Digital IDs.
Regulation 5: Fingerprints	Fingerprints are taken by officials at Department offices or approved processes.	Retain Department control. The draft's private-sector enrolment model must not permit banks or other private staff to collect,

Provision	Holistic concern	LFN comment / requested amendment
		view, store, transmit or reuse fingerprints for the State.
Regulation 6 / proposed regulation 37: Change of address and contact particulars	The current regulation requires notification by prescribed form and, in certain circumstances, written consent before the Director-General records a change. The draft permits *MyMzansi*, accredited trusted entities and updated mobile/email details.	The draft must not dilute the consent safeguard. Changes through trusted entities must require express consent, non-digital confirmation, and a right to contest. Mobile numbers and email addresses should not become mandatory for physical-ID users.
Regulation 7: Certificates	Birth, marriage and death certificates remain official documents.	Digital ID must not replace or undermine paper certificates. Courts, schools, hospitals, banks and public bodies must continue to accept lawful physical certificates.
Regulation 9: Application for identity card	A person must apply for an identity card within 30 days after attaining 16 years.	This physical-ID duty must not be conflated with a Digital ID duty. Any communication to young persons must clearly state that Digital ID is voluntary. The provision should

Provision	Holistic concern	LFN comment / requested amendment
		refer to a natural living human being or individual where appropriate.
Regulation 10: Temporary identity certificate	The current framework provides temporary identity certificates.	A non-digital temporary identity certificate and emergency paper fallback must remain available where Digital ID fails, is suspended, is unavailable, or the individual lacks a device.
Regulation 11: Steps to ensure application for identity card	Failure to comply with a request to apply for an identity card is an offence.	The offence must apply only to lawful physical identity-card duties under the Act, and never to failure or refusal to apply for, activate or use a Digital ID. It must also be clear that the duty relates to natural living human beings, not juristic persons or non-human systems.
Regulations 12 to 14: Amendment, cancellation, replacement and duplicates	The current framework allows surrender, seizure, cancellation and replacement of physical identity cards/certificates.	The amended Regulations must distinguish between physical-document cancellation and Digital ID suspension/revocation. A Digital ID dispute must not automatically contaminate the physical ID, and vice versa, unless authorised by the Act and supported by reasons.

Provision	Holistic concern	LFN comment / requested amendment
Regulation 15: Fees and furnishing of information	Current regulation 15(d) allows furnishing information from the population register in real-time or batch format to any person, organisation, body, society or institution for a fee.	This is the most important holistic defect. It must be rewritten so that paid verification cannot bypass the trusted-entity, consent, purpose-limitation, logging and *POPIA* safeguards. No person or entity should be able to purchase population-register information outside a strict rights-protective framework.
Existing regulation 16 / draft regulations 47 and 48: Offences	The draft repeals the old general offence and inserts new offences.	The draft contains cross-reference errors and overbreadth. It must protect citizens from private-entity misuse as strongly as it penalises citizens for misuse. Refusal to use Digital ID must never be an offence or indirect offence.
Annexures	The current Annexures are designed for paper-based processes.	The Annexures must be updated with privacy notices, consent wording, *POPIA* rights, non-digital fallback information, and warnings that Digital ID is voluntary. Where forms refer to "*person*", "*applicant*" or "*holder*", they should distinguish natural living human beings from entities where necessary.

6. Structural Defects in the Draft Amendment Scheme

6.1. Excessive Reliance on Future Instructions

6.1.1. The draft repeatedly permits the Director-General to determine important standards and particulars by instruction. Examples include mandatory particulars, secure presentation means, renewal steps, biometric standards, fingerprint use, liveness standards, device certification, cryptographic standards, API standards, mobile-device security and accreditation forms.

6.1.2. LFN accepts that technical standards may require periodic updating. However, rights-affecting matters may not be shifted out of public comment and into later unpublished or lightly published instructions. Matters such as what information is mandatory, who may access it, whether biometrics may be queried, how private entities participate, when "*person*" means a natural living human being, and what citizens can refuse must be contained in the Regulations themselves.

6.1.3. LFN requests that all instructions with rights implications be published in draft form for public comment before the Regulations are finalised, alternatively that the Regulations expressly require public consultation before any instruction that expands data categories, access rights, trusted-entity powers or biometric processing.

6.2. Current Regulation 15(d) May Bypass the New Framework

6.2.1. Regulation 15(d), as currently in force, allows a fee for furnishing information from the population register on magnetic tape or similar format in accordance

with section 21(2) of the Act, including real-time verification and batch verification to any person, organisation, body, society or institution.

6.2.2. The draft amendments create a narrower trusted-entity framework, yet do not expressly repeal or rewrite regulation 15(d). This produces a serious loophole. If “any person, organisation, body, society or institution” can continue to buy real-time or batch population-register verification, then the trusted-entity safeguards, data-sharing agreements, audit duties and consent principles may be undermined.

6.2.3. LFN requests that regulation 15(d) be rewritten so that no furnishing of population-register information, whether real-time, batch, magnetic tape, API, or similar format, may occur except under the same consent, *POPIA*, *PAIA*, audit, purpose-limitation, data-minimisation, public-register and redress safeguards applicable to trusted entities. Preferably, regulation 15(d) should be deleted and replaced by a comprehensive access-and-fee provision aligned with regulations 32 to 38A.

6.3. Ambiguous Use of “Person” Creates Human-Identity and Non-Human Entity Risks

6.3.1. The draft repeatedly uses the word “*person*” in contexts dealing with Digital ID credentials, biometric data, liveness detection, identity enrolment, identity verification, identity assurance levels, population-register particulars, ordinary residence, applications, renewals, suspensions, revocations and proof of identity. In ordinary legal drafting the word may be understood from context, but in a Digital ID framework the risk of ambiguity is materially higher.

6.3.2. South African law, including the *Interpretation Act* does not confine "*person*" to a living human being. It may include juristic persons, companies, bodies corporate, unincorporated associations and other *personae fictae*. The draft itself also introduces "trusted entities", vendors, accredited enrolment points, APIs, mobile devices and automated verification infrastructure. The result is a mixed human/entity/digital environment in which loose use of "person" is unsafe.

6.3.3. LFN further submits that the modern environment creates an additional risk. There are already debates, in South Africa and abroad, about whether human-like rights or legal recognition may be extended to artificial intelligence systems, robots, digital agents, software modules, machine identities and other non-human constructs. Whether one agrees with those debates or not, human identity legislation must not accidentally create ambiguity that could later become an unnecessary obstacle to administration or litigation.

6.3.4. A Digital ID credential is tied to a living human being's biometrics, dignity, privacy, bodily integrity, civic status, ordinary residence and access to public services. A company, trust, municipality, voluntary association, bank, AI module, robot, digital wallet, device, account, corporate profile or machine identity cannot rationally have a human face, fingerprint, liveness, bodily integrity, human dignity, ordinary residence in the human sense, or civic particulars in the population-register sense.

6.3.5. LFN accordingly requests that the Regulations define "individual" or "natural living human being" and then use that term wherever the subject is the holder, applicant or data subject of a human identity credential. The word

"*entity*" should be used where juristic persons, trusted entities, organs of state, vendors, banks, mobile operators or institutions are intended. This will prevent both ordinary statutory ambiguity and future attempts to stretch human identity infrastructure to *personae fictae* or non-human automated systems.

6.4. Private-Sector Enrolment Converts Commercial Institutions into Proxy State Agents

6.4.1. The draft allows private-sector enrolment points through accredited trusted entities. In practical terms, this includes entities such as banks and mobile operators, because the definition of trusted entity expressly includes entities with statutory identity-verification duties relating to anti-money-laundering, electronic communications and other regulated activities.

6.4.2. The result is that commercial institutions may collect, confirm, transmit and refresh citizens' identity particulars while influencing identity-assurance levels. This is constitutionally dangerous. A bank may verify its own client for *FICA*. It should not become an outsourced Home Affairs office, biometric collector, assurance-level contributor or population-register update channel.

6.4.3. If private premises are used for convenience, the process must remain a Department process performed by Department personnel, with Department equipment and no access, retention or reuse by the private host.

6.5. Technical and Drafting Errors Must Be Corrected

6.5.1. The *Gazette* notice heading refers to the Identification Act, 2002 (can possibly refer to the 'Animal Identification Act, 2002'), which creates confusion, while the body refers to the Identification Act, 1997. This must be corrected to avoid uncertainty.

6.5.2. Regulation 33(1) skips paragraph (e). This must be corrected.

6.5.3. Regulation 44(g) refers to compliance audits in accordance with regulation 37, while audit requirements are in regulation 36. This must be corrected.

6.5.4. Regulation 48(1)(h) refers to regulation 45(e), but regulation 45 has no paragraph (e). The intended reference appears to be regulation 44(e).

6.5.5. Regulation 48(2) states that a person convicted of an offence in terms of regulation 49(1) is liable to punishment. This appears to be a cross-reference error; it should refer to regulation 48(1).

6.5.6. Regulation 47 criminalises contravention of regulations 4 to 15, but not regulation 3. If regulation 3 is excluded deliberately, the reason must be stated. If not, the provision must be corrected.

6.5.7. Regulation 50 says the Regulations shall be called the Identification Regulations, 2026. Since the legal instrument is an amendment to the Identification Regulations, 1998, the Department must clarify whether it is replacing the principal Regulations or merely amending them. The short title should not create confusion.

6.5.8. The drafting must distinguish "person", "individual", "holder", "applicant", "data subject", "trusted entity", "accredited entity", "vendor", "organ of state"

and “juristic person” with precision. Without this, the Regulations may produce avoidable interpretive disputes.

7. Specific Objections and Requested Amendments

7.1. Objection 1: Digital IDs Must Never Become Mandatory in Law or Practice

7.1.1. LFN welcomes the wording that a person “may, but is not required to” apply for a Digital ID. However, the true danger is indirect compulsion. Digital IDs may become mandatory if banks, mobile operators, employers, schools, insurers, municipalities, licensing offices, hospitals, security estates, airlines, courts or service providers refuse to deal with physical IDs.

7.1.2. The Regulations must therefore bind both public and private actors. An individual must be able to use a physical ID book/card in all situations where a Digital ID would otherwise be accepted, unless an Act of Parliament expressly and constitutionally authorises a particular limitation.

7.1.3. “*Voluntary*” must mean voluntary in everyday life, not merely voluntary inside the Department’s own application form.

7.2. Objection 2: Physical IDs Must Remain Equal and Permanent

7.2.1. The physical identity book/card system must remain operational, affordable, accessible and equally accepted. It must not be treated as legacy, inferior or transitional.

7.2.2. The State must maintain non-digital channels for applications, renewals, corrections, address changes, certificates, temporary identity certificates, duplicates and dispute resolution.

7.2.3. Any proposed discontinuation or degradation of physical IDs must require primary legislation, a socio-economic impact assessment, full public participation and parliamentary oversight.

7.3. Objection 3: Biometrics of Physical-ID Users Must Be Segregated from Digital-ID Infrastructure

7.3.1. LFN recognises that the current physical-ID framework already involves photographs and fingerprints. That does not mean those biometrics may be exposed to Digital ID systems, facial-recognition engines, liveness detection tools, APIs, private vendors or trusted entities for individuals who have not chosen Digital ID.

7.3.2. An individual who chooses physical ID only must remain outside the Digital ID ecosystem to the maximum extent technically and legally possible.

7.3.3. Biometric processing must be minimised, segregated, encrypted, access-controlled, independently audited and subject to user-visible logs.

7.4. Objection 4: Consent Must Be Specific, Informed, Recorded and Transaction-Based

7.4.1. Data-sharing agreements between the Department and trusted entities do not amount to consent by citizens. A citizen is not a party to that agreement.

LFN objects to the State and a private institution deciding between themselves how a citizen's identity data will flow.

7.4.2. The default model should be user-present, transaction-specific verification. The trusted entity should receive the minimum possible response, preferably a yes/no confirmation or cryptographic proof, not raw personal data.

7.4.3. Consent must not be bundled into bank terms, mobile contracts, employment onboarding, insurance applications or app terms. Refusal of Digital ID data sharing must not result in refusal of service where a physical-ID route exists.

7.5. Objection 5: Trusted Entities and Verified Relationships Are Too Broad

7.5.1. The definition of trusted entity is wide enough to include many state, *quasi*-state and private bodies. Regulation 38A then allows verified relationships and near real-time update notifications. This architecture creates a continuous identity-data mesh around the citizen.

7.5.2. LFN objects to near real-time update notifications to private entities unless each specific notification is demonstrably necessary, consented to by the citizen, and required by a clear statutory duty.

7.5.3. The Department must not create a standing identity-surveillance ecosystem in which every address, mobile number, email address or mandatory particular flows between the population register and commercial institutions.

7.6. Objection 6: Identity Assurance Levels Must Not Create a Two-Tier Citizenry

7.6.1. Regulation 24 allows identity assurance levels to increase when a person is verified by accredited trusted entities. This may sound technical, but it can create a hierarchy between “high-trust” and “low-trust” citizens.

7.6.2. Wealthier, urban, banked and digitally active persons may accumulate higher assurance. Poor, rural, elderly, unbanked, privacy-conscious or physical-ID-only citizens may be treated as lower assurance. That would offend equality and dignity.

7.6.3. Assurance levels must never be used as a generalised citizen score, eligibility condition, service-quality differentiator, credit-risk indicator, fraud suspicion marker, or basis for differential treatment. They must be internal, transaction-specific and not disclosed unless strictly necessary and consented to.

7.7. Objection 7: No Racial, BBBEE or Sensitive Classification

7.7.1. LFN objects to any Digital ID, identity number, QR code, machine-readable expression, digital wallet, API response, identity-assurance level, verified relationship or population-register interface storing, displaying, encoding, inferring, transmitting or facilitating access to race, ethnic origin, colour, BBBEE classification, employment-equity classification, health status, vaccination status, political persuasion, religious or philosophical belief, trade union membership or comparable sensitive classification.

7.7.2. Even where other legislation permits certain entities to collect demographic information for their own statutory reporting, such data must remain external

to national identity credentials. An identity credential must prove identity. It must not become a racial tag, BBBEE token, health passport or social-control instrument.

7.7.3. LFN requests an express exclusion clause in the Regulations, because relying on silence is insufficient.

7.8. Objection 8: "Person" Must Be Limited to a Natural Living Human Being Where Human Identity Is Concerned

7.8.1. LFN objects to the repeated use of the word "person" in the current and proposed Regulations without sufficient precision. In South African law, "person" may include *personae fictae* and not only natural human beings. This creates avoidable ambiguity in a regulatory framework concerned with human biometrics, liveness detection, identity cards, population-register particulars and access to public services.

7.8.2. This concern is not academic. The proposed Digital ID framework also deals with trusted entities, accredited entities, private institutions, vendors, APIs, mobile devices, automated verification systems and digital credentials. Unless the Regulations expressly distinguish human beings from non-human entities, future disputes may arise as to whether certain rights, identity features, access routes or legal statuses may be extended to juristic persons, AI modules, software agents, robots, machine identities, digital wallets, accounts, devices or other artificial constructs.

7.8.3. LFN's position is that Digital ID credentials under these Regulations must be limited to natural living human beings whose particulars are or may lawfully

be included in the population register. No juristic person, *persona ficta*, company, trust, organ of state, municipality, association, body corporate, unincorporated body, artificial intelligence system, software module, digital agent, robot, automated system, digital wallet, device, account, corporate profile, machine identity or other non-human entity may apply for, hold, present, use, activate, renew, benefit from or be recognised as the holder or bearer of a Digital ID credential issued under these Regulations.

7.8.4. LFN accordingly requests that the Regulations define “individual” as a natural living human being and thereafter replace “person” with “individual”, “natural person”, “applicant”, “holder” or “data subject” wherever the subject is a living human being. Conversely, where the Regulations intend to refer to banks, companies, organs of state, municipalities, vendors, trusted entities or other institutions, they must use “entity”, “trusted entity”, “juristic person”, “body”, “organ of state” or “institution”.

7.8.5. This definitional clarity is necessary *ex abundanti cautela* to prevent both ordinary statutory misinterpretation and any future ideological or technological attempt to extend human biometric identity infrastructure to non-human entities.

7.9. Objection 9: Suspension and Revocation Require Strong Redress

7.9.1. Regulation 21 allows suspension for suspected fraud, pending contact re-verification, failure to comply with obligations, or where suspension is otherwise necessary. The phrase “otherwise necessary” is too broad.

7.9.2. If a Digital ID becomes widely used, suspension may lock a person out of life. The Regulations must provide reasons, non-digital notice, urgent objection, human review, independent complaint mechanisms, physical-ID fallback and compensation for wrongful harm.

7.9.3. No person's physical ID may be suspended, cancelled or treated as suspect merely because a Digital ID has been suspended, unless the Act expressly permits it and written reasons are supplied.

7.10. Objection 10: Public Participation Is Inadequate

7.10.1. The comment period of approximately 33 days is inadequate for a national biometric identity framework affecting every person in South Africa.

7.10.2. The Department should publish the full draft regulatory scheme, draft instructions, draft data-sharing agreements, impact assessments, cybersecurity summaries, operational-readiness reports and plain-language summaries before requesting final comment.

7.10.3. A new comment period of at least 60 days must follow, with publication of the draft Regulations and a plain-language explanatory summary in all written official languages, together with accessible formats for persons with disabilities, including screen-reader compatible documents, large-print versions, and, where public briefings or explanatory videos are used, South African Sign Language interpretation.

7.11. Objection 11: Operational Readiness and Cybersecurity Must Be Proven

7.11.1. A national biometric identity system is high-risk infrastructure. If it fails, citizens may be excluded. If it is breached, faces and fingerprints cannot be changed like passwords.

7.11.2. The Department must publish or table an independent operational-readiness and cybersecurity certificate before commencement. Where technical details cannot be made public for security reasons, an independent public executive summary must still be provided.

7.11.3. The Regulations must include uptime standards, disaster recovery, manual fallbacks, breach notification, compensation, vendor liability, staff vetting, false-match and false-rejection testing, and independent audits.

7.12. Objection 12: Function Creep Must Be Expressly Prohibited

7.12.1. LFN objects to Digital ID infrastructure being used for purposes unrelated to identity verification voluntarily initiated by the person concerned.

7.12.2. The Regulations must prohibit use for e-voting, social-credit scoring, vaccine-status enforcement, health-status disclosure, protest monitoring, political profiling, debt collection, automated fines, commercial analytics, targeted advertising, race-based profiling and generalised surveillance.

7.12.3. Any future expansion must require new legislation or, at minimum, new regulations with proper public participation and parliamentary oversight.

8. Consolidated Proposed Clauses

8.1. LFN proposes that the following clauses be inserted in substance. The Department may refine numbering and technical drafting, but not dilute their constitutional effect.

Definition of individual:

"*individual*" means a natural, living human being whose particulars are or may lawfully be included in the population register, and excludes any juristic person, *persona ficta*, company, trust, organ of state, municipality, association, body corporate, unincorporated body, artificial intelligence system, software module, digital agent, robot, automated system, digital wallet, device, account, corporate profile, machine identity or other non-human entity.

Interpretative clause:

For the purposes of these Regulations, any reference to an applicant, holder, identity-card holder, data subject, individual or person in relation to a digital identity credential, biometric data, liveness detection, identity enrolment, identity verification, identity assurance level, identity card, population-register particulars, ordinary place of residence, proof of identity, suspension, revocation or renewal shall mean a natural living human being only, unless the Regulation expressly refers to a juristic person, trusted entity, accredited entity, organ of state or other institutional body.

Exclusion of non-human identity claims:

No juristic person, *persona ficta*, company, trust, organ of state, municipality, association, body corporate, unincorporated body, artificial intelligence system, software module, digital agent, robot, automated system, digital wallet, device, account, corporate profile, machine identity or other non-human entity may apply for, hold, present, use, activate, renew, benefit from or be recognised as the holder or bearer of a digital identity credential issued under these Regulations.

Voluntariness and equal legal effect:

No individual is required, directly or indirectly, to apply for, hold, present, use, activate, renew or rely upon a digital identity credential. A valid physical identity book, physical identity card, temporary identity certificate, certificate issued under the Act, and digital identity credential shall be accepted equally for all lawful purposes of proof of identity, and no individual may be disadvantaged for choosing any one lawful identity format over another.

Anti-discrimination by public and private actors:

No organ of state, public body, private body, trusted entity, accredited entity, service provider, accountable institution, mobile operator, financial institution, employer, educational institution, healthcare provider, municipality, insurer, landlord or any other person may refuse service, impose additional conditions, levy higher fees, delay service, reduce benefits, lower assurance, or treat an individual adversely solely because that individual uses a valid physical identity document instead of a digital identity credential, or *vice versa*.

Physical fallback:

Every service, transaction or administrative process for which proof of identity is required must maintain a physical, non-digital and offline verification route that is reasonably accessible, affordable and not materially inferior to a digital route.

Regulation 15(d) alignment:

No information from the population register may be furnished in real-time, batch format, magnetic tape, API, or any similar format to any person, organisation, body, society, institution, trusted entity or accredited entity except in accordance with *POPIA*, *PAIA*, these Regulations, a lawful and specific purpose, data minimisation, audit logging, retention limits, breach notification, and the data subject's clear, specific, informed, voluntary and recorded consent, save where disclosure is expressly required by an Act of Parliament, warrant, court order or other lawful authority applicable to that specific disclosure.

No private-sector biometric collection for the State:

No private entity may collect, process, retain, transmit or verify biometric data on behalf of the Department for purposes of enrolment for a digital identity credential, unless such processing is performed exclusively by Department personnel, on Department-controlled systems, with no access, retention or reuse by the private entity.

Biometric segregation for physical-ID users:

Where an individual does not hold or use a digital identity credential, that individual's biometric data may not be made accessible through digital identity credential systems, trusted-entity verification services, API interfaces, assurance-level scoring, verified-relationship records or update notifications, save where expressly authorised by an Act of Parliament, court order or warrant.

Consent-based data sharing:

No information from the population register may be furnished to a trusted entity unless the data subject has given clear, specific, informed and recorded consent for the particular transaction and the particular categories of information to be disclosed, save where disclosure is expressly required by an Act of Parliament, court order, warrant or other lawful authority applicable to that specific disclosure.

No racial or sensitive classification:

No digital identity credential, machine-readable expression, API response, assurance level, verified relationship, QR code, digital wallet or data-sharing arrangement may contain, infer, display, encode, transmit or facilitate access to race, ethnic origin, colour, BBBEE classification, employment-equity classification, health status, vaccination status, political persuasion, religious or philosophical belief, trade union membership or comparable sensitive classification.

User audit rights:

Every individual shall have a free, accessible and non-digital means to obtain a full record of all accesses, verification queries, disclosures, update notifications and trusted-entity interactions relating to his or her information, including the identity of the requester, date, time, purpose, legal basis, data categories accessed, outcome and retention period.

No function creep:

Digital identity infrastructure may be used only for identity verification and authentication necessary for the transaction voluntarily initiated by the individual concerned, and may not be used for social-credit scoring, political profiling, protest monitoring, e-voting, vaccine-status enforcement, race-based profiling, commercial advertising, credit scoring, debt collection, automated fines, generalised surveillance or any purpose not expressly authorised by law after public participation.

Redress and human review:

No adverse decision affecting access to identity, services, benefits, banking, communications, employment, education, healthcare, voting, travel, licensing or lawful economic activity may be made solely by automated processing. Affected individuals must receive reasons, non-digital notice, access to urgent human review, an independent complaint mechanism, and a physical-ID fallback pending final determination.

9. Requests

9.1. LFN requests that the Minister and the Department not finalise the draft amendments in their current form.

9.2. LFN requests that the draft amendments be withdrawn, alternatively materially amended and republished, to include the following:

9.2.1. An express definition of “individual” as a natural living human being only, excluding juristic persons, personae fictae, artificial intelligence systems, software modules, robots, digital agents, automated systems, digital wallets, devices, accounts, corporate profiles, machine identities and other non-human entities.

9.2.2. A full review of the Regulations to replace “person” with “individual” or “natural person” wherever the subject is a living human being, and to reserve “entity”, “trusted entity”, “juristic person”, “body”, “organ of state” or “institution” for non-human legal or institutional actors.

9.2.3. An express anti-compulsion and anti-discrimination clause binding both public and private actors.

9.2.4. Permanent equal status and practical acceptance of physical ID books/cards, temporary identity certificates and lawful certificates.

9.2.5. A non-digital, offline fallback route for every identity-dependent service.

9.2.6. Deletion or strict limitation of private-sector enrolment points and trusted-entity biometric roles.

9.2.7. Rewriting of regulation 15(d) so that paid real-time or batch access to population-register information cannot bypass the new safeguards.

9.2.8. Deletion or major narrowing of regulation 32(2)(d), especially the phrase "*such other lawful purposes as may be specified in a data sharing agreement*".

9.2.9. Deletion or major narrowing of regulation 38A on verified relationships and near real-time update notifications.

9.2.10. Clear, specific, transaction-based consent as the default for any State-private identity-information exchange.

9.2.11. Express prohibition on race, BBBEE, employment-equity, health, vaccine, political, religious and comparable sensitive classifications in Digital ID infrastructure.

9.2.12. Biometric segregation for persons who choose not to hold or use Digital IDs.

9.2.13. Independent cybersecurity and operational-readiness certification before commencement.

9.2.14. User-visible audit logs and non-digital access to records of all queries and disclosures.

9.2.15. Rapid redress, human review, physical-ID fallback and compensation for wrongful suspension, false matches, breaches or administrative error.

9.2.16. Correction of drafting errors, cross-reference errors and the incorrect *Identification Act* reference in the *Gazette* notice.

9.2.17. Publication of all draft instructions, data-sharing templates, impact assessments and plain-language summaries before any finalisation.

9.2.18. A fresh public-comment period of at least 60 days, with publication in all written official languages and accessible formats for persons with disabilities.

10. Conclusion

10.1. LFN repeats that Digital ID may be useful when it is a voluntary convenience. It becomes constitutionally dangerous when it becomes a condition of daily life, a private-sector data pipeline, a biometric surveillance layer, a racial or sensitive-classification instrument, a human/non-human identity ambiguity, or a mechanism that quietly downgrades those who prefer physical identification.

10.2. Having now considered the current Identification Regulations, 1998, together with the proposed amendments, LFN submits that the existing and proposed regimes must be reconciled before finalisation. The Department cannot responsibly finalise the Digital ID provisions while leaving older population-register access mechanisms, physical-ID rules, address-change rules, offence provisions, fee-based data-sharing provisions and definitional ambiguities insufficiently harmonised with the new privacy and rights safeguards.

10.3. A Digital ID framework that affects human dignity, privacy, bodily integrity, biometrics and civic identity must be drafted with absolute clarity that it applies only to natural living human beings, and not to juristic persons, artificial systems, digital agents, robots or any other non-human entities. If South Africa ever chooses to regulate digital agents, AI modules, robots, machine identities or corporate identity systems, that must be done in separate legislation after separate public participation, not by ambiguity in human identity Regulations.

10.4. LFN accordingly requests that the Department withdraw the draft amendments in their current form, alternatively amend and republish them in line with this submission. LFN requests written reasons if any material request herein is rejected.

10.5. LFN reserves all rights *in toto*, including the right to request records under *PAIA*, to make further submissions, to participate in parliamentary processes, and to institute review proceedings should the final Regulations remain constitutionally defective.

Yours Faithfully,

Reyno D. De Beer

President: Liberty Fighters Network

On behalf of our members and acting in Public Interest