



ID4AFRICA 2025
IDENTITY REGULATORY
FRAMEWORK FOR SOUTH AFRICA
DATE: 21 MAY 2025



home affairs
Department:
Home Affairs
REPUBLIC OF SOUTH AFRICA



Confidential

We Care!

KEY DRIVERS IN REFORMING IDENTITY MANAGEMENT

The need to modernize South Africa's legal framework for identity management has been driven by several key signs and systemic challenges, many of which have become more urgent due to technological, security, and socio-political factors. Here are the main drivers:

1. Fragmented and Outdated Legal Framework

- These laws have not kept pace with digital transformation, biometric technologies, and integrated government services.

2. Increased Identity Fraud and Corruption

- The ease with which identity documents could be forged or fraudulently obtained led to widespread identity theft, social grant fraud, and illegal access to public services.

3. Inefficient Public Service Delivery

- Lack of interoperability between government databases impedes efficient service delivery and social planning.

4. Need for Inclusion and Constitutional Rights.

- The identity system needed to align more closely with the constitutional right to dignity, equality, and access to services.

5. Digital Transformation and e-Government Goals

- The South African government has increasingly moved toward digital government and smart service delivery (e.g., e-health, e-education).

6. Security and National Planning.

- A modern ID system was needed to better manage migration, border control, and national statistics.

PROCESS OF REFORMING IDENTITY MANAGEMENT

- The identity management reform process in South Africa has followed a multi-phase, consultative, and policy-driven approach, largely led by the **Department of Home Affairs (DHA)**. The aim has been to modernize, digitize, and unify the country's identity system in a way that aligns with constitutional values and global best practices. Here's an overview of the **key steps and processes followed** in this reform:
 - **Policy Development and Diagnostic Review**

The process began with a **comprehensive review** of the existing identity management systems, highlighting fragmentation, legal inadequacies, inefficiencies, and risks such as fraud. This led to the development of the **Identity Management Policy**, published for public comment in 2021.
 - **Public Consultation and Stakeholder Engagement**

The DHA initiated an **inclusive consultative process** involving:

 - Civil society organisations
 - Academia and researchers
 - Legal experts
 - Government departments (e.g., Health, Education, Social Development)
 - ICT sector and private stakeholders
- Feedback from these engagements shaped the policy framework to ensure it was rights-based, inclusive, and technologically relevant.
- The **National Identification Registration Bill** is currently being finalised before its signed into law.



home affairs

Department:
Home Affairs
REPUBLIC OF SOUTH AFRICA



We Care!

❑ **DHA White Paper**

Through this White Paper, the DHA is positioning itself to deliver effectively against its mandate as a critical enabler of citizen empowerment, economic development, national security and an efficient state.

❑ **Identification Act (ID Act)**

The ID Act provides the foundations for the establishment of the population register and issuing of enabling identification documents to qualifying citizens and residents and will be replaced by a new identification management legislation.

❑ **Protection of Personal Information Act, (POPIA)**

The POPIA on the other hand, prescribes the grounds for lawful processing of personal information from private and public sector actors. The POPI Act sets out the minimum standards regarding accessing and ‘processing’ of any personal information belonging to another. The Act defines ‘processing’ as collecting, receiving, recording, organizing, retrieving, or the use, distribution or sharing of any such information.

❑ **Cybercrimes Act 19 of 2020**

The Cybercrimes Act 19 of 2020 is an official Act of Parliament. The Act has created twenty cybercrime offenses including unlawful access to a computer or data storage device, illegal acquisition or interception of data, the unlawful acquisition, receipt, or possession of a password, as well as online forgery, extortion, or fraud and is the overarching legal authority on the regulation, investigation and criminalization of cybercrimes.



❑ **Section 14 of the Constitution of the Republic of South Africa**

The Fourth Amendment Protects the right of privacy against unreasonable searches and states that everyone has the right to privacy, which includes the right not to have— (a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communications infringed.

❑ **The Electronic Communications and Transactions Act 25 of 2002.**

The objective of ECTA is to provide for the facilitation and regulation of electronic communications and transactions and to prevent the abuse of information systems. The ECTA applies to all persons and entities that make use of (i.e. send and receive) electronic communications and data messages.

❑ **Draft National Data and Cloud Policy**

The Draft Policy seeks to create an enabling environment for the provision of data and cloud services in an effort to move “towards a data intensive and data driven South Africa” that ensures social and economic development and inclusivity

❑ **Draft Policy proposal relates to;**

- *Digital infrastructure*
- *Cloud computing infrastructure*
- *Data protection, data localization and cross boarder transfers*
- *Cybersecurity measures*



- ❑ A policy and regulatory landscape that protects privacy, addresses systemic risk, and establishes a legal framework for digital ID is a necessary foundation for the program to be a success. Aligning digital identity systems for compliance with national framework and policies is an imperative.

- ❑ **The Trust Framework**

A digital identity system must be built on a foundation of trust if it is to generate widespread acceptance among users that unlocks revenues in value added services, while also helping governments achieve the related sustainable developmental goals.

- ❑ The roles that both government and the private sector might play in the identity realm raise important issues of regulatory policy relating to trust.

- ❑ As a result, Research suggests that robust ‘trust frameworks’ need to be built by aligning several components of digital identity creation, including ***the technical specifications, standards and procedures, data protection, privacy and other identity-related laws, regulations, and consumer expectations***

The combination of these elements is often referred to as a ‘trust framework’.



❑ **Digital Citizenship Policy**

The Digital Citizenship policy is intended to help all users of the network understand what individuals should know in order to use technology in a meaningful, responsible and respectful manner.

- ❑ Digital citizenship refers to the ability to think critically, behave safely, and participate responsibly in our digital world. Too often citizens misuse and abuse technology. The issue is more than what the users do not know but what is considered appropriate technology usage.
- ❑ The move to digitize government services and transactions between individuals and government agencies elevates digital identity to a new level of commercial and legal significance.
- ❑ These factors make analysis of the functions and legal nature of digital identity in a transactional context important and timely, and the framework that encapsulate all these factors is referred to as a Digital Citizenship Policy.



THANK YOU



home affairs

Department:
Home Affairs
REPUBLIC OF SOUTH AFRICA

Confidential



We Care!
8