

# SELF-SERVICE SMART ID MACHINES IN SOUTH AFRICAN BANKS: WHAT IT MEANS IN TERMS OF POPIA

Category: Privacy Law and POPIA, Privacy Law, Infosec, and POPIA  
written by Nolitha Mrwata | March 23, 2026



## Self-service Smart ID Machines in South African Banks: What it Means in terms of POPIA

On 9 March 2026, the Department of Home Affairs launched its first self-service Smart ID terminals, allowing citizens to apply for Smart ID documents within selected bank branches. Participating banks, including Capitec and Standard Bank, now allow citizens to apply for Smart ID cards through dedicated terminals located in their branches. This initiative forms part of the Department's broader digital transformation strategy aimed at expanding access to government services and reducing congestion at traditional Home Affairs offices. Under this model, citizens can visit participating bank branches in which the system allows banks to connect directly to the department's systems through a secure digital gateway where trained staff will assist them with Smart ID applications and biometric verification.

While the initiative promises improved convenience and efficiency, it also raises important questions relating to the protection of personal information, particularly considering the Protection of Personal Information Act ("**POPIA**").[\[1\]](#)

### Is the decentralisation of this system a good idea?

From a service delivery perspective, decentralising Smart ID applications to banks could significantly improve accessibility for citizens. Banks already possess sophisticated digital infrastructure and identity verification systems, which may support faster processing and more reliable authentication.

However, the involvement of banks in the collection and processing of biometric data introduces additional data protection considerations. Biometric information is classified as special personal information, which requires heightened safeguards and stricter conditions for processing under POPIA.[\[2\]](#)

## **The implications for biometric data processing**

Organisations processing personal information must comply with several key POPIA principles, including:

- Purpose specification – personal information must be collected for a specific, explicitly defined purpose.[\[3\]](#)
- Data minimisation – only information that is necessary for the stated purpose may be collected.[\[4\]](#)
- Security safeguards – responsible parties must secure the integrity and confidentiality of personal information.[\[5\]](#)
- Accountability – organisations remain responsible for ensuring compliance with POPIA.[\[6\]](#)

In the context of Smart ID applications within banks, biometric data is captured to verify identity and facilitate the issuing of identification documents. In terms of section 10 of POPIA, this data must only be processed for its intended and lawful purpose and must not be retained or used beyond what is necessary for that purpose.

### **Safeguards banks must implement**

Banks participating in this initiative must ensure that adequate safeguards are in place to protect the personal information of citizens. These safeguards may include:

- Strict access controls to biometric data systems;
- Clear data retention policies; and
- Proper staff training on data protection obligations.

Failure to implement appropriate safeguards could expose institutions to regulatory scrutiny and potential liability under POPIA.

### **A step in the right direction - but with caution**

The integration of Smart ID services within bank branches represents a significant step toward modernising public service delivery in South Africa. If implemented correctly, it has the potential to make government services more accessible and efficient.

However, the success of this initiative will ultimately depend on whether participating institutions can effectively balance innovation with robust data protection practices. As biometric technologies become more integrated into everyday service, strict compliance with POPIA will be essential to maintaining public trust and safeguarding the personal information of South African citizens.

---

[\[1\]](#) Protection of Personal Information Act (hereinafter “POPIA”)

[\[2\]](#) Section 26 of POPIA

[\[3\]](#) Section 13 of POPIA

[\[4\]](#) Section 10 of POPIA

[\[5\]](#) Section 19 of POPIA

[\[6\]](#) Section 8 of POPIA