MYMZANSI AND THE RISE OF DIGITAL IDS: CAN SOUTH AFRICA BALANCE INNOVATION WITH PRIVACY?

Category: IT Law,Privacy Law and POPIA,Technology Law
written by Ethan Van der Merwe | August 19, 2026

On 4 May 2026, Dr Leon Schreiber, the Minister of Home Affairs, gazetted draft amendments to the Identification Regulations of 1998, made under the *Identification Act* 68 of 1997. These proposed amendments contemplate the use of digital IDs in South Africa which can be used on your smartphone.

Dr Schreiber has suggested that the proposed rollout of these digital IDs will assist the Department of Home Affairs ("**the Department**") to crack down on the rampant fraud in physical IDs, an issue which is particularly pertinent when it comes to the ID book.[1]

In the draft amendments, the Department has outlined the establishment and the usage of digital IDs which are to be stored on South Africans' smartphones and will be valid in the same way as your current physical smart ID card is today.[2] It should be noted that this system does not seek to replace the current physical smart ID cards and shall be completely optional. However, the digital IDs will be used to access government services and facilitate digital payments.[3]

The use of these digital IDs has created some cause for concern amongst South Africans, particularly as it relates to cybersecurity and personal data protection. The Department has highlighted several essential security measures for the digital IDs, however, with the current rise in cybersecurity breaches in South Africa, the concern remains a very significant one.

Kaspersky has warned that any data stored on mobile devices can be exposed through malicious applications.[4] With the advance of capabilities employed to gain illicit access to information stored on smartphones, strong protections are required to protect such sensitive personal information.

According to Kaspersky, the risks range from simpler phishing techniques to far more innovative measures such as trojans, which present themselves as legitimate, harmless applications, but have the ability to take over an authentication app to gain access to ID credentials.[5]

The Department has taken important strides to ensure the security of the digital IDs. Some of the measures put forward to protect the personal information include the requirement of biometric authentication to establish and access digital IDs. Digital IDs will not appear as visual documents but will instead appear as data that can be accessed via QR codes, NFC tags, and Bluetooth. Device binding, which ensures that, should login credentials be compromised, the device on which the information is stored will be required to gain access. Finally, cryptographic signatures will be implemented to ensure the identity credentials' authenticity.[6]

These security measures are comprehensive and admirable; however, a key question arises: how secure is the personal information? The Department has suggested that the digital IDs will be stored on MyMzansi, an app to be designed to provide citizens with digital access to various government services. The MyMzansi app is set to be designed by the Digital Service Unit ("**DSU**") within the Presidency of South Africa. Beyond the ever-existing risk of the compromise of the digital ID itself is the risk of additional personal information stored through the MyMzansi app. We await to see the app's privacy policy and its steps to protect additional personal information which may be accessed.

The implementation of digital IDs and the MyMzansi app will involve the processing of extensive personal information, including special personal information in the form of biometric data. The Department, as a responsible party as contemplated in the Protection of Personal Information Act 4 of 2013 ("**POPIA**"), will be required to ensure compliance with the conditions for lawful processing contained in POPIA, including security safeguards, purpose specification, data minimisation, and accountability. Of particular importance and consideration will be section 19 of POPIA, which requires the Department to secure the integrity and confidentiality of personal information through appropriate technical and organisational measures.

The MyMzansi app may ultimately become a central repository of personal information associated with an individual's interactions with government services. Its key function is to provide digital access to government services, which will require more personal information than just one's ID. The MyMzansi app will likely have additional personal information which may include passport details, driver's license information, residential addresses, telephone numbers, email addresses, tax information, pension records, unemployment benefits, social grant or welfare records, and the list goes on. The information stored by the app will be subject to which features are to be added, but should the app's purpose be for digital access to government services, it is imaginable that all of the above personal information will be stored by the app. Beyond the comprehensive security measures directed around digital IDs, what security measures will be used to protect MyMzansi itself?

The implementation of the digital ID and the use of the MyMzansi app must be balanced against the constitutional right to privacy. The State has a legitimate objective in combatting fraud and improving service delivery, however, the collection and processing of personal information must remain proportionate to those objectives and compliant with POPIA.

Now, what about the biometric information?

Biometric information is of great value in ensuring the protection of digital IDs. If done right, when biometrics are stored and processed properly, they're safer than many other forms of authentication.[7] However, where will this information be stored? Apps primarily make use of two types of storage methods, namely on-device storage or cloud storage.[8] Generally speaking, an on-device storage method is the more secure manner of storing your biometrics largely due to the fact that such information is not uploaded to a server where the risk exists that the encryption mechanisms used on the cloud server are not properly implemented.[9] Cloud storage is a more convenient option, however, it is more vulnerable to hacks and it runs the risk of services not using robust encryption.[10]

This is not to say that, should MyMzansi elect to store biometric information in the cloud, there will be a breach of personal information. If done in the correct way, such as through the use of the Advanced Encryption Standard ("**AES**"), personal information will be stored in a highly secure manner.[11] AES is a symmetric block cipher which was chosen by the United States National Institute of Standards and Technologies to protect electronic data.[12] AES ensures that should your data be compromised, it remains unreadable without the decryption key.[13] What is therefore required, should DSU implement cloud storage of biometric data, is the proper implementation of strong encryption mechanisms.

There is currently a shift towards on-device storage. The key advantage of the on-device storage option is that biometric data never leaves your device.[14] Your biometric data remains encrypted on your device and is not stored on a server, making it less vulnerable to hacks.

Consequently, what will be of the utmost importance with the MyMzansi app will be its privacy policy and the cybersecurity mechanisms it will employ to protect your personal information. Beyond the digital ID, a vast quantity of personal information will be stored and processed by the app. In light of the growing cyberattacks which have occurred against South African institutions, many eyes will be on the proactive security measures to be taken by the DSU in the creation of the MyMzansi app.

The Department's proposed digital ID framework is a significant step towards the modernisation of public services in South Africa. Should it be successfully implemented, digital IDs have the potential to reduce fraud, streamline interactions with government, and improve access to essential services. However, the success of the project revolves around public trust. Clear governance structures, comprehensive cybersecurity measures, transparency regarding the collection and storage of personal information, and strict compliance with POPIA will be essential to securing public trust. We will be keeping a keen eye on these developments to ensure that innovation is matched by equally strong protections for privacy and data security.

---

[1] Security concerns about South Africa's plans for a Digital ID Book – MyBroadband

[2] Ibid.

[3] Ibid.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] How to Use Biometric Authentication Safely

[8] Ibid.

[9] Ibid.

[10] Ibid.

[11] Ibid.

[12] Advanced Encryption Standard (AES)

[13] Op cit note7.

[14] Ibid.