WERKSMANS
ATTORNEYS

REGULATORY

How SIM cards and open Wi-Fi allegedly exposed the SANDF's data weaknesses

17 October 2024 *3 min read*

The South African National Defence Force ("**SANDF**") plays a critical role in safeguarding South Africa's sovereignty and territorial integrity.[1] As the backbone of South Africa's defence infrastructure, the SANDF processes vast amounts of personal information, but also classified information essential to its operations, intelligence and planning.

Given this crucial function, the SANDF is expected to maintain the highest level of security when it comes to protecting its data systems. However, there have been recent allegations that its data systems were "compromised" by an installer's SIM cards and open access Wi-Fi.[2]

It was reported that –[3]

- the computer management system that backs up all the military's internal databases had been compromised after a contractor installed SIM cards and open access via Wi-Fi on the nationwide relay systems; and
- defence intelligence raided the relay stations to remove the microchips and SIM cards.

Whether or not an actual "compromise" occurred, this incident underscores the importance of implementing robust security safeguards as required in terms of the Protection of Personal Information 4 of 2013 ("**POPIA**"). In particular, section 19 of POPIA specifically requires responsible parties (in this instance, the SANDF) to take "*appropriate, reasonable technical and organisational measures*" to prevent –

- loss of, damage to or unauthorised destruction of personal information; and
- unlawful access to or processing of personal information.

In this instance, the allegation that the SANDF's national data systems were compromised by an installer's SIM cards and open access Wi-Fi suggests a weakness in the security framework of the SANDF and potentially exposes the SANDF to data breaches, unauthorised monitoring and/or even espionage which could have far-reaching consequences for national security.

Consequently, implementing appropriate security safeguards as required by POPIA such as, amongst others, encrypted communication channels and restricted access to networks is critical to protect and ensure the security of personal information. This alleged "compromise" demonstrates the urgent need for organisations, particularly those processing special personal information or those in high-security environments (like the SANDF) to proactively assess and enhance their security safeguards and data protection policies and procedures. Failing to comply presents risk from a POPIA perspective, but also (in this instance) puts national security at risk.

> *"There are only two types of companies: those that have been hacked and those that will be."*
>
> ***Robert S. Mueller, Former FBI Director***

The Werksmans Data Privacy and Cyber teams aim to empower clients in establishing robust security architecture and posture. In particular, we conduct data protection impact assessments as required in terms of POPIA in order to reveal weaknesses in security safeguards.

[1] See the website of the Department of Defence at http://www.dod.mil.za/about, accessed on 11 October 2024.

[2] See the City Press article titled "SANDF national data systems 'compromised' by installer's SIM cards and open access Wi-Fi" available at https://www.news24.com/citypress/news/sandf-national-data-systems-compromised-by-installers-sim-cards-and-open-access-wi-fi-20240915, accessed on 11 October 2024.

[3] See the City Press article titled "SANDF national data systems 'compromised' by installer's SIM cards and open access Wi-Fi" available at https://www.news24.com/citypress/news/sandf-national-data-systems-compromised-by-installers-sim-cards-and-open-access-wi-fi-20240915, accessed on 11 October 2024.

Ahmore Burger-Smidt

Head of Regulatory

View Profile

Dale Adams