WERKSMANS
ATTORNEYS

REGULATORY

Cybersecurity Breaches vs The SABS Breach of "Standards"

19 December 2024 *7 min read*

Issues of maladministration and mismanagement at the South African Bureau of Standards ("**SABS**") have been the subject of much contestation in the recent months and consequently, the reason behind the Department of Trade, Industry and Competition's ("**DTIC**") investigation of the SABS' officials. Further inflaming these issues, was the recent cybersecurity breach that affected most of the SABS' core operations, and which commands the question of whether the SABS does in fact, *develop, maintain and promote national standards*... in line with its mandate.

In November 2024, the SABS experienced yet another cybersecurity breach – a third one within a period of a year, with previous incidents reported in 2023 and also in April this year[1]. It is reported that the recent ransomware attack crippled the SABS' IT systems, leaving operations at a standstill, from certification processes to employee salaries.

It is also reported that the recent breach occurred after several interventions and expenditure of R140 million including capital expenditure of R9.5 million for improved IT security[2]. Consequently, the DTIC has been called upon to expand the scope of its on-going investigation into the SABS, to make provision for immediate independent audits of the SABS cybersecurity expenditure and current cybersecurity status.

However, whilst issues relating to allegations of the SABS' misappropriation of the funds allocated for its cybersecurity system enhancements may be the main subject of the proposed independent audits, the DTIC and/or appointed independent auditors ought not be oblivious of the data privacy implications of the incessant cybersecurity breaches.

These cybersecurity breaches raise pertinent questions relating to the SABS' compliance with the Protection of Personal Information Act 4 of 2013 ("**POPIA**"), more specifically with the conditions for the lawful processing of personal information.

The first question that comes to mind is whether the SABS has taken 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.

as required in terms of section 19(1) of POPIA.

To give effect to the above obligation, the SABS must have taken reasonable measures to –

- identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- establish and maintain appropriate safeguards against the risks identified;
- regularly verify that the safeguards are effectively implemented; and
- ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards[3].

Burns and Burger-Smidt provide a useful explanation of this requirement, by way of the following data breach scenario –

"Company A became a victim of a cyberattack. Through the attack, access is gained to user accounts and there is an attempt to withdraw funds from the accounts. Obviously these attackers access the personal data associated with the various accounts.

What would enable such an attack? Deficiencies in the security measures companies take to secure customers' data, include:

- *insufficient password policy and user authentication; and*
- *insufficient control measures to validate changes to a user's account.*

Various steps can be taken to mitigate the abovementioned. These steps could include, inter alia:

- *implementation of passwords which require more than one factor;*
- *implementation of a comprehensive data retention policy; and*
- *implementation of a login alert system."* **[4]**

Therefore, in consideration of the above and the fact that the SABS has been a victim of repeated cybersecurity breaches, the DTIC's investigation should include, within its scope, an inquiry of whether the SABS' latest enhancements to its cybersecurity system, *if any,* were appropriate to prevent the loss of, damage to, or unauthorised destruction of personal information and unlawful access to or processing of personal information. Furthermore, whether the safeguards implemented, albeit recently infiltrated, respond to the deficiencies in previously implemented safeguards.

A further and more important question that follows is whether the SABS notified the Information Regulator and the affected data subjects of the cybersecurity breach.

POPIA requires that where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party (in this instance, the SABS) must notify the Information Regulator and the data subject[5].

The notification must provide sufficient information to allow the affected individuals to take protective measures against the potential consequences of the data breach, including –

- a description of the possible consequences of the data breach;
- a description of the measures that the responsible party intends to take or has taken to address the data breach;
- a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the data breach; and
- if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information[6].

The significance of the obligation to notify of data breaches is also demonstrated by a further report, that according to the South African National Accreditation System requirements, the SABS is obliged to inform its clients about the loss of data and the potential risk of a cybersecurity breach[7].

Of particular relevance to the POPIA considerations discussed above is the Enforcement Notice issued by the Information Regulator against Dis-Chem Pharmacies Limited ("**Dis-Chem**")[8] for breaching the conditions for the lawful processing of personal information and failing to comply with the duty to notify of security compromises.

In terms of the Enforcement Notice, Dis-Chem was ordered by the Information Regulator, *inter alia,* to –

- conduct a Personal Information Impact Assessment to ensure that adequate measures and standards exist to comply with the conditions for the lawful processing of personal information;
- ensure that the appropriate security safeguards that are put in place include, but are not limited to, the implementation of an adequate Incident Response Plan which addresses the following –
    - Preparation and Prevention;
    - Detection and Analysis;
    - Containment and Eradication; and
    - Recovery and Post Incident Activities.

- ensure that an appropriate Incident Response Plan that makes provision for all aspects of POPIA, Cyber Crimes Act and other related legislative frameworks applicable to the protection of personal information is developed; and
- develop, implement, monitor and maintain a compliance framework, in terms of Regulation 4(1)(a) of POPIA which clearly makes provision for the reporting obligations of Dis-Chem and all its operators in terms of section 22 of POPIA.

In the event of the SABS being found to be non-compliant with sections 19 and 22 of POPIA, an Enforcement Notice against the SABS on terms that are similar to the Dis-Chem Enforcement Notice seems probable. However, each case is decided on its own merits.

A bureau of standards failing to uphold standards? A lesson that, indeed, a book cannot and *should not* be judged by its cover.

---

[1] See the Engineering News article titled "Major SABS cyberattack raises questions about entity's leadership" available at https://www.engineeringnews.co.za/article/major-sabs-cyber-attack-raises-questions-about-entitys-leadership-2024-12-03, accessed on 12 December 2024.

[2] See the Business Day article titled "Bureau of Standards officials probed" available at https://bd.pressreader.com/article/281487871934681, accessed on 11 December 2024.

[3] See section 19(2) of POPIA.

[4] See Burns Y and Burger-Smidt A (2023) *Protection of Personal Information: Law and Practice, 2nd edition: LexisNexis.*

[5] See section 22 of POPIA.

[6] See section 22(5) of POPIA

[7] See the Engineering News article titled "Major SABS cyberattack raises questions about entity's leadership" available at https://www.engineeringnews.co.za/article/major-sabs-cyber-attack-raises-questions-about-entitys-leadership-2024-12-03, accessed on 12 December 2024.

[8] Reference number: SC 30/2022

Ahmore Burger-Smidt

Head of Regulatory

View Profile

Lwazi Mtshilibe

Senior Associate

View Profile