WERKSMANS
ATTORNEYS

REGULATORY

# Data breaches in South Africa post POPI...Any lessons to be learned?

2 September 2020 *6 min read*

*by Ahmore Burger-Smidt, Director and Head of the Data Privacy Practice; and Dale Adams, Candidate Attorney*

1. During mid-August 2020, social media, news reports and other online platforms was awash with news that approximately 23.4 million South Africans' personal information was compromised. The data breach was announced by Experian South Africa ("**Experian**") on 19 August 2020 in a statement to the effect that:

> *"Our investigations indicate that an individual in South Africa, purporting to represent a legitimate client, fraudulently requested services from Experian. The services involved the* ***release of information which is provided in the ordinary course of business or which is publicly available****".[1] [Emphasis added]*

2. Following this incident, Experian South Africa stated that:

- the authorities including, National Credit Regulator and the Information Regulator, and other major stakeholders were notified; and
- the perpetrator of this data breach was apparently identified and an *Anton Piller* order was obtained against him which effectively "*impounded*" the hardware and software used to carry out the data breach. Furthermore, the misappropriated data was secured and deleted.[2]

3. Correctly, Experian issued a notification to the Information Regulator, but is this enough?

4. Experian stated that "*no consumer credit or consumer financial information was obtained*", but what information was then the subject of the breach?

5. We are unclear as why a period of approximately three months expired prior to the announcement of the actual data breach. We also cannot comprehend whether such information was divulged elsewhere prior to Experian taking cognizance of the data breach.

6. Sadly, the above is one of the "known" four major data breaches in South Africa in the preceding eight months of 2020 alone, and will, no doubt, not be the last data breach for 2020. Unfortunately, this worrying increase in data breaches does not correlate with an increase in preparedness by companies. In fact, many companies are woefully underprepared.

7. The financial impact of a data breach is undoubtedly one of the most immediate and hard-hitting consequences that companies will have to deal with. There are clear examples of companies having faced significant financial damage post a data breach. This is exactly what happened to Yahoo after it was confronted with a data breach in 2013. The breach only became known in 2016 when the company was about to be bought over by US telecoms company Verizon. The acquisition went ahead with the company buying Yahoo doing so at a discounted rate of an estimated amount around $350 million less than the original asking price.

8. Research demonstrates that the costs associated with data breaches continue to rise. The problem with cyber-attacks is that no matter how much you do to combat them, there is always a good chance that one may happen. If we consider phishing scams and other malicious communications, we know that these invite devastating attacks and are introduced by employees! Phishing scams are typically sent as emails that prompt users to click on a malicious link loaded with spyware or malware that allows the bad actor to siphon off data from the company's network whenever they please. Combatting these attacks requires equipping employees with tools, education, and training as this will help companies to defend against these threats in the future. Furthermore, not having in place robust processes to be followed prior to releasing personal information poses a risk and can contribute to the risk of releasing personal information to someone you think you know.

9. The so-called silver-lining to these data breaches have accentuated the need for robust legislative dictates applicable to businesses which process personal information. The Protection of Personal Information Act 4 of 2013 ("**POPI**") clearly spells out the expectations of the Information Regulator once a data breach occurs.

## What does POPI stipulate?

10. POPI seeks to give effect to the right to privacy enshrined in section 14 of the *Constitution of the Republic South Africa*, 1996. The preamble of POPI posits that the right to privacy includes the right to protection against the unlawful collection, retention, dissemination and use of personal information. POPI places an obligation on companies to process personal information responsibly and this includes the protection against data breaches.

11. POPI provides that a responsible party, which is defined as a person or business which processes personal information, will be obliged in the event of a data breach to notify the Information Regulator as well as affected parties within a reasonable time after the discovery of the compromise. Section 22 of POPI provides that the notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including the following:

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

## Conclusion

12. The undeniable reputational and financial harm arising from a data breach is significant, in addition to the disruption that a data breach may have to a business's operations. The provisions of POPI relating to data breaches will strengthen the hands of the authorities to fight against data breaches in South Africa, but this is not enough.

13. Responsible parties must ensure that they have an appropriate data breach response plan in place. This data response plan must comply with the notification requirements contained in section 22 of POPI. Responsible parties must take it upon themselves to train and equip staff about POPI and the dangers associated with data breaches.

> The Werksmans POPI e-learning course provides a comprehensive tool for businesses and employers to train and equip staff to deal with POPI and the inevitable risk of data breaches in South Africa and how to protect against data breaches.

---

[1] Statement by Experian dated 19 August available at https://www.experian.co.za/fraudulent-data-incident, accessed on 23 August 2020.

[2] *Ibid.*

**Ahmore Burger-Smidt**

Head of Regulatory

View Profile