WERKSMANS
ATTORNEYS

REGULATORY

Data breaches: to notify, or not to notify, that is the question

6 October 2021 *6 min read*

Data breaches

We have had a number of clients approach us on the issue of security compromises or "data breaches" and have quickly come to learn that a similar theme or question permeates throughout this issue. That is whether to notify the data breach to the Information Regulator ("**Regulator**") and data subjects concerned, and if so, when.

The concept of a data breach is not formally defined in the Protection of Personal Information Act, No. 4 of 2013 ("**POPIA**") which presents challenges for businesses trying to determine whether something constitutes a data breach or not. However, the wording of section 22 of POPIA can provide some much-needed guidance in this regard. Section 22 of POPIA provides that:

> *"(1) 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, must notify–*
>
> *(a) the Regulator; and*
>
> *(b) subject to subsection (3), the data subject, unless the identity of such data subject cannot be established." [Emphasis added]*

Section 22(3) of POPIA

Section 22(3) of POPIA provides for an exception to the above provision and states that:

> *"The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned."*

- *Accessed or acquired*

Section 22 of POPIA refers to the personal information of a data subject being "accessed" or "acquired". The Oxford Advanced Learner's Dictionary defines "access" to mean –

> *"the opportunity or right to use something or see somebody/something."*

It then defines "acquire" to mean –

> *"to gain something by your own efforts, ability or behaviour"; or*
>
> *"to obtain something by buying or being given it."*

- *Unauthorised*

Unauthorised, as per its dictionary definition, means –

> *"without official permission."*

Section 22(1) of POPIA

Consequently, section 22(1) of POPIA envisions a situation where a person lacking official permission acquires or is provided with the opportunity to see or use another person's personal information.

What this means is that instances of data breaches can range from nefarious acts such as hackers gaining access to a system or server containing personal information or innocent acts of negligence or mistakes such as an employee of a business inadvertently sending personal information to an unauthorised third party. Both acts fall within the meaning of a data breach within the South African context as they involve a person lacking official permission gaining access or being given the opportunity to see or use another person's personal information.

This creates a challenge for businesses and the Regulator. On the part of businesses, it means that every instance of data breaches, regardless of its consequence, must be notified to the Regulator and the affected data subjects. This presents risks of reputational damage and fractured relationships with customers even where a breach may result in no adverse consequence. On the part of the Regulator, it means that it may become inundated with notifications for breaches which may not even warrant any further action or intervention due to their inconsequential nature.

Article 33(1) of the General Data Protection Regulation 2016/679 ("GDPR")

This is a position that is contrary to international practice, in particular that of the European Union ("**EU**") and the United Kingdom ("**UK**"). Article 33(1) of the General Data Protection Regulation 2016/679 ("**GDPR**"), which is the data protection law that is applied across the EU, provides that:

> *"In the case of a personal data breach, the controller [responsible party] shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay." [Emphasis added]*

From the above, we get the concept of a 'breach without consequence'. In short, what this is means is that where a data breach results in no risk to the rights and freedoms of data subjects, it need not be notified to the relevant regulatory authority. A similar position is held in the UK as confirmed by its regulatory authority (Information Commissioner's Office).[1]

Having in place a threshold to determine whether it is necessary to notify to a data breach presents both practical and commercial benefits. Businesses would not have to run the risk of suffering significant reputational harm by notifying inconsequential breaches and the Regulator would not have to be inundated by what can only be imagined to be a barrage of inconsequential breaches coming out of businesses.

However, this carve-out is not available to responsible parties in terms of POPIA which means that each and every data breach must be notified irrespective of whether it has adverse consequences or not.

Section 22(5) of POPIA

This applies even where the personal information concerned is in an encrypted form. We highlight this because some businesses try to put forward encryption as a method of escaping the responsibility to notify. However, this factor does not exempt a responsible party from notifying a data breach. It may only serve as a factor to include in the content of the notification in terms of section 22(5) of POPIA which we discuss in more detail in a separate article discussing **what should go into a data breach notification**.

This section dictates that the notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise. In other words, knowing that the personal information is in an encrypted form may allay fears of it being actually accessed and used by unauthorised parties. However, the fact that such parties are in possession of the personal information is enough to trigger the notification requirement.

Consequently, it is important for all businesses to take note of the fact that where personal information held by them has been accessed or acquired by an unauthorised party, a data breach has occurred which should be notified to the Regulator and data subjects concerned. A failure to adhere to this may open them up to receiving an administrative fine should they fail to comply with an enforcement or information notice.

Notification of data breaches… setting the record straight – read more.

---

[1] See, for example, https://ico.org.uk/for-businesses/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/, accessed on 22 September 2021.

by Ahmore Burger-Smidt, Director and Head of Data Privacy and Cybercrime Practice and member of the Competition Law Practice and Nyiko Mathebula, Candidate Attorney

Ahmore Burger-Smidt

Head of Regulatory

View Profile