WERKSMANS
ATTORNEYS

REGULATORY

When the walls fall in

5 October 2022 *3 min read*

Ring-a-round the rosie, A pocket full of posies, Ashes! Ashes! We all fall down

The Information Regulator has officially made her presence known. The Enforcement Committee has been established and we have noted various announcements from the Office of the Information Regulator as to current actions underway.

But what does this mean to each and every company? What does this mean to comply with POPIA[1] and how does this impact compliance initiatives? In short, what tasks can employees perform, with absolutely no ill intent, that can still bring the wall falling down?

Can't make head or tail of POPIA? Lessons from Sheburi V Rail Safety Regulator – Read more here

Employees are expected to remember and adhere to numerous policies, including privacy policies. Poster campaigns are rolled out to reinforce positive behaviour and still when we consider data breaches it is often unbelievable how the mistake that resulted in the breach could have possibly occurred. The reality is that many data breaches occur when employees believe they are doing the right thing.

The top 5 employee privacy risk potholes to avoid.

Employees DO NOT be too helpful!
Employees want to do the right thing to keep customers, suppliers, internal and external clients happy. However, being overly helpful may result in an employee providing unnecessary information to complete a task, which increases the risk of a data breach. For example, a well-intended employee may provide more personal information than required. If that information is provided to unauthorised individuals, it would result in a data breach which would be required to be notified to the Information Regulator.

Security rules are not followed!
When employees are in a rush and under work pressure, it happens that information, personal information and confidential information could be sent out without applying password protection or using proper encryption. This problem occurs when the security processes and technology is too difficult and time consuming to use, or alternatively the employee has not been trained and cannot use the technology solutions properly.

Sending files to the incorrect recipient!
This is in fact the most common and difficult issue to tackle at a company. Many email applications automatically store past email addresses. However, this can increase the chances of a mistake as employees may use the incorrect auto-filled email address and fail to double-check the recipient's name. It is only after the email is sent, or when the recipient notifies the sender of the incorrect transmission that the error is discovered.

The risk of multi-tasking
We are all busy with more than one computer monitor and have a number of computer applications open at a time. When personal information is entered into the wrong system and disclosed this results in a data breach!

They collect what they DO NOT need!
Only asking for the bare minimum relevant information required is key and employees must consider this carefully. The less personal information a company has and employees have access to, the less the risk of a data breach. Logically the converse applies.

A lack of robust business processes and employee POPIA training cannot be underestimated.

Thinking before you do, must be the rule when it comes to employees and privacy. Let the house stand firm!

Footnotes

[1] The Protection of Personal Information Act, No. 4 of 2013

Ahmore Burger-Smidt

Head of Regulatory

View Profile