POPIA - A cost-effective starting point

August 2018
Without Prejudice

South Africa has suffered numerous data breaches in recent months, and although the Protection of Personal Information Act, 2013 (POPIA) is only partially in effect, the Information Regulator has urged both public and private companies to comply with their data protection obligations in terms of POPIA.

According to *Sunday Times*, following the data leak on the ViewFines website, the Information Regulator had written a letter to the website owner, Aggregate Payment Systems, reminding it of its obligations in terms of POPIA. The recent Liberty Life breach also saw the Information Regulator requesting the extent and contents of the data breach, interim measures put in place to prevent further breach and whether those affected by the breach had been informed – all being notification requirements in terms of POPIA.

While South Africa still finds itself on the back foot with regard to the regulation of data privacy and protection, draft regulations are currently under consideration by the Information Regulator suggesting that the dawn of POPIA could be drawing much closer. POPIA is substantially based on the UK Data Protection Act and obliges compliance within a year of it coming into effect. But a year to comply with a global standard is highly unlikely to be sufficient. Depending on the environment, an assessment and implementation, on average, are likely to take anything between 12–36 months. Failure to comply can give rise to severe consequences, including an uncapped claim for civil damages against the responsible party, a maximum imprisonment of 10 years and/or a fine of not more than ZAR10 million, depending on the circumstances of the breach. On this basis, it is clearly important that businesses get a head start on POPIA compliance. But where do we start?

In the absence of POPIA being in full force and effect, a good starting point for implementation, is section 19(1), which requires several appropriate, reasonable organisational and technical measures to be implemented to safeguard personal information. Although this will have a significant impact on businesses financially, as various security measures, policies and procedures will need to be reassessed and improved upon to ensure an appropriate standard of safety and security, financial constraints should not be a justification for non-compliance. Especially when it comes to the safeguarding of personal information in this era, where data breaches are rife. This then leaves businesses struggling with finding an appropriate balance between compliance and the availability of finances.

A possible solution of how cost implications can be reduced, surprisingly leads to an area already covered by POPIA, namely section 19(2). POPIA is not only our first comprehensive piece of legislation on data privacy and protection, but also the first to require a risk register to be kept. How then does this make a business's implementation of POPIA cost-effective? Well, identifying what risks you have before implementing safeguard measures will essentially enable you to identify the areas in which security measures will be necessary and the type of security measures needed. The standards for compliance with POPIA are clearly reflected in section 19(1), requiring appropriate, reasonable measures to be taken. A thorough assessment of a business's environment will indicate what is appropriate and reasonable in the circumstances. On this basis, you need not adopt every measure available, but rather the necessary measures that are appropriate and reasonable to your environment and the risks identified. Those tasked with safeguarding and securing the personal information used are, however, cautioned against adopting measures that they deem appropriate and reasonable in the absence of consulting experts in the relevant areas. These include compliance, legal and information technology experts. Businesses should also consider any applicable industry standards in implementing their safeguards. What always needs to be borne in mind is that the solution must be fit for purpose.

While POPIA does make a distinction between personal information and special personal information (the latter being subject to more extensive requirements for use and includes personal information such as religious affiliations, race and health information), responsible parties should be cautious not to detract from the importance of appropriately safeguarding personal information, since even disparate pieces of personal information, coupled with other personal information obtained from another source, could be used to an individual's detriment.

The consequences of non-compliance and obligations to constantly monitor the systems in place, as required by the risk register in terms of section 19(2) of POPIA, should be more than sufficient to persuade those tasked with safeguarding personal information, that compliance with POPIA can never be a simple "tick-box" exercise. To avoid not only the consequences for non-compliance in terms of POPIA, but also reputational risks associated therewith, businesses should already have started planning, preparing and safeguarding themselves well in advance, before POPIA comes into full force and effect.

> Read the full article online