Nikki Pennel

Associate Director
Data Protection Law
Tel: +27 82 719 5916
Email: nikki.pennel@kpmg.co.za

Data privacy

Key regulatory challenges emerging from POPIA and the GDPR

Has anything really changed?

It has been almost six years since the Protection of Personal Information Act of 2013 ("POPIA") was promulgated and a year since the European Union's General Data Protection Regulations ("GDPR") came into effect. While POPIA still awaits an effective date for the provisions which require compliance from the entities processing personal information, there remains a heightened global focus on privacy as a fundamental consumer right.

In South Africa, the Policy Holder Protection Rules (for both the long term and short term insurance industries) dovetail with the requirements of POPIA insofar as confidentiality, privacy, security and retention of data is concerned, with the provisions relating to data management coming into effect on 1 January 2020.

The South African Information Regulator has officially occupied office since 1 December 2016. Notwithstanding that the substantive provisions of POPIA are not yet effective, the Information Regulator has informally been handling various complaints received from consumers and has been engaging with companies who have been the subject of material information security breaches. The Information Regulator has convened meetings with various government institutions, including the HAWKS, the National Prosecuting Authority, the National Credit Regulator and the Credit Bureau Association and other foreign data protection authorities, such as the United Kingdom's Information Commissioner Office.

A level of uncertainty remains insofar as the extent to which companies should already be implementing the requirements of POPIA from a consumer relations perspective, with certain service providers to insurers refusing to take any tangible steps towards compliance until an effective date for POPIA is announced. This places insurers in an unenviable position of balancing the longstanding relationships they may have with their key service providers with the need to provide a customer-centric service offering to their clients.

The GDPR remains high on the agenda

Globally, the GDPR remains high on the agenda for insurers, but it appears that the approach to compliance remains primarily reactive and uncoordinated. Mark Thompson, KPMG's Privacy Advisory Lead has remarked that "this often stems from the issue that it is not owned at the board level, where the board form a clear articulation of the organisation's privacy risk appetite, which is then translated into a risk-based remediation plan. This is surprising for a sector with risk management at its core." ("Privacy and the GDPR – Have you got it right?" The London Journal, 2018).

In South Africa, most insurers have done something in the way of data protection, either from a POPIA perspective or in terms of global policy which compels the incorporation of the GDPR into their action plans. However, true compliance remains a challenge. In certain instances, privacy gap analyses or impact assessments, which were conducted some years ago in response to the promulgation of POPIA in 2013, are still being relied upon with little implementation having been completed other than changes to key policies and contracts and ensuring that cybersecurity risks are managed.

Compliance requirements which require human intervention or which require fundamental changes to data management processes, particularly relating to the insurer's duty of transparency and obligation to provide access to personal information, remain problematic.

We set out below some of the key challenges that have emerged within the South African privacy / data protection landscape.

Key emerging challenges

Consent management

Consent is but one of the lawful justifications for processing of personal information. However, relying on consent as a justification for processing personal information potentially creates an additional administrative burden under both POPIA (and the GDPR). This is due to the specific requirement for consent under POPIA (and the GDPR) - that is, it cannot be implied and must be voluntary, specific and informed. In order to meet this requirement, any notice which an organisation uses to inform its data subjects of the nature and purpose of processing personal information must be sufficiently specific for data subjects to be in a position to provide such informed consent.

As data subjects may withdraw their consent at any time (subject to the provisions of section 11(2)(b) of POPIA), there is a need for insurers to put in place a process which enables them to manage consents and withdrawals of consent and respond accordingly.

Data subject requests

While data security remains top of mind in the context of data protection and privacy, the management of personal information insofar as access requests, deletion and portability are concerned is a significant challenge for financial services firms.

On 14 December 2018, the South African Information Regulator published the relevant forms to be used when a data subject wishes to request a correction or deletion of personal information in terms of POPIA. Few South African companies, however, have established formal processes through which such requests may be received and actioned across the organisation and the systems it uses. At best, requests for personal information have been handled on an ad hoc basis, without a complete understanding of the personal information retained by the insurer (in its various forms) about that individual.

While subject access requests might not currently be a burning issue for South African insurers, it should be noted that after the GDPR came into effect, the insurance industry in the United Kingdom experienced a 20% increase in subject access requests within a period of a week. Once South African consumers are alerted to their rights of access to their own personal information, a similar increase can be expected.

Management of third party vendors

The use of third party service providers to process personal information, such a tracing agents, credit bureaux, forensic investigation services and other service providers, are potential areas of risk. POPIA requires that all responsible parties (organisations which determine the purpose and means of processing personal information) ensure, through a written contract that its third party "operators" (persons who process person information for an on behalf of the responsible party), establish and maintain the relevant security measures referred to in POPIA.

Beyond the contractual requirement which POPIA imposes on responsible parties, the extent to which financial services companies should have insight into their third party "operators'" specific security measures and be involved in the monitoring of their compliance, will need to be considered in the context of the nature and volume of personal information being processed by the "operator" concerned. Additional monitoring processes will further add to the financial services firms' administrative burden, but will be necessary in order to manage its risk exposure and protect the rights of its customers.

Reporting obligations under the Cybercrimes Bill

Related to information security and privacy, financial institutions will need to be aware of the obligations which are sought to be placed on them under the current version of the Cybercrimes Bill.

The Cybercrimes Bill seeks, amongst other things, to impose obligations on electronic communications service providers and financial institutions to report cybercrimes and provide technical and other assistance to the police in their investigations of cybercrime.

Concluding remarks

Despite the lengthy hiatus since the promulgation of POPIA, other (and perhaps more urgent) drivers compel a renewed focus on privacy and responsible data management in the insurance industry. According to a KPMG survey (as published in The London Journal 2018) of nearly 7000 individuals globally, nearly 75% of respondents have low levels of trust in insurance organisations that process their personal data, with just 7.7% indicating that they trust insurers completely. This is in stark contrast when compared to banks, with 40% of respondents indicating that they have high levels of trust in banks processing their personal data.

These statistics should raise alarms with senior executives across the insurance sector, as in the absence of trust, customers are likely to be increasingly resistant to share their personal information, potentially undermining future insurance business models and strategies.

The imminent changes to the South African consumer protection landscape and the enforcement market conduct will require organisations to develop a thorough understanding of their privacy and data security risks and controls to identify those areas where additional efforts are required to strengthen the effectiveness of their programmes. This is necessary, both for the sake of managing the legislative risk involved and cultivating customer trust in this industry.