The POPI Act

DOWNLOAD ARTICLE

The Protection of Personal Information Act, 2013, or "POPI" as it has colloquially become known, promotes the protection of personal information by requiring that public and private bodies comply with certain standards when collecting, processing, storing and sharing personal information.

This Act is set to become effective towards the end of 2018, once the regulations have been promulgated, and has been described as a compliance disruptor of the highest order. There is absolutely no doubt that this piece of legislation has become necessary and indeed laudable, keeping us in line with overseas trends. In the preamble to the Act, the legislators weigh up the situation as follows in justifying the promulgation of the POPI Act:

"**IT IS RECOGNISED THAT** Section 14 of the Constitution of the Republic of South Africa 1996, provides that everyone has the right to privacy;

that the right to privacy includes a right to protection against unlawful collection, retention, dissemination and use of personal information;

that the State must respect, protect promote and fulfil the rights in the Bill of Rights.

BEARING IN MIND THAT consonant with the constitutional values of democracy and openness, the need for economic and social framework of the information society, requires the removal of unnecessary impediments to the free flow of information, including personal information.

AND IN ORDER TO regulate in harmony with international standards the processing of personal information by public and private bodies in a manner that gives effect to the right of privacy subject to justifiable limitations, aimed at protecting other rights and important interests."

Whilst the Act comes from Canada, the concepts of thesis, antithesis and synthesis can be identified from the early Greek philosophers. The thesis could be interpreted to be the right to privacy, the antithesis would be, the need for streamlined economic progress and quick transfer of information, and the synthesis, otherwise known as agreed middle ground, would be the POPI Act which balances all stakeholder interests.

So, we all agree that the core purpose of the Act is to ensure that individuals and juristic persons know exactly what is being done with their personal information.

In the context of Sectional Title, there are two groups of people to hone in on. The first are the individuals or companies owning units in a Sectional Title Scheme. Management Rule 27(2)(b) states that:

"The Body Corporate must prepare and update the following records:

List of Trustees, members and tenants with:

- Full names
- ID Numbers (non-citizens must provide passport numbers)
- Section address
- E-mail address
- Telephone numbers"

More importantly, and increasingly controversial is Management Rule 27(4):

"On receiving a written request, the Body Corporate must make the records and documents referred to in the rule available for inspection by, and provide copies to:

a. a member;

b. a registered bondholder;

c. a person authorised in writing by a member or registered bondholder.

Management Rule 27(5) states that "The Body Corporate must comply with a request for inspection or copying under this rule within 10 days.

This in effect means that any owner can insist upon receiving personal information about another owner, just as long as he makes the request in writing.

My feeling is that this Rule may well be in contravention of the POPI act unless the rule includes a consent provision, and an amendment of the Management Rule may have to be looked at.

The second group of people affected in our Industry, are Managing Agents, as they receive and collect volumes of personal information about schemes and residents. Personal information would include payroll data. CV applications for employment, CCTV TV records, performance reviews of employees and communication information such as internal e-mails between owners, or between owners and the Managing Agents.

It is important at this juncture to mention that the POPI Act prohibits the processing of "special personal information." This covers information about a person's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, criminal behaviour or biometric information. Quite a pity really, as our complexes constitute fertile ground for substantially interesting information under 'special personal information' (said tongue-in-cheek).

The POPI Act will provide challenges to the business of the Managing Agent.

Once the Act becomes effective, there will be a 12 month implementation timeframe. The body overseeing the enforcement of the law will be the Information Regulator. The Chairperson of the Regulator has advised that companies must immediately start working on the following:

1. An awareness process for staff members.
2. A Promotion of Access to Information Act Manual update (PAIA)
3. Internal system to process requests.
4. The appointment of an Information Officer.
5. A compliance framework.

Managing Agents should identify the specific types of personal information to be collected, and should not make the mistake of over collecting irrelevant information, or keeping any information once their mandate is terminated. They should be cautious about further processing limitations. An example of this is where personal information was originally created to manage a specific building. Then, it became an attractive option to utilise that information to promote an ancillary product, being financing a scheme, or landscaping within a scheme. It is critical that the Managing Agent establish that owners have agreed to the further processing. Over and over the collection of information, it cannot be over emphasised enough that the quality of captured information should be of a high standard. The Companies Information Officer at the Managing Agent must be able to confirm that reasonable and practical steps were taken to ensure that personal information was complete, accurate and up to date.

Another direct question an Information Officer will be hard pressed to answer is what the company is doing to prevent unlawful access to or unlawful processing of personal information. This is the hard question that Liberty Life is dealing with currently.

Managing Agents, will need to think about how to secure the integrity and confidentiality of personal information and, furthermore, to consistently update new risks or deficiencies. Both internal and external risks to personal information under the Agents control should be identified, and policies with regard to the use of flashdrives, external hard drives and other storage devices will have to be worked on and bedded down.

An interesting section of the Act for owners and Managing Agents deals with Direct Marketing. Section 69 of the Act outlaws direct marketing by means of any form of electronic communications has to disclose the identity of the advertiser and provide an address to which the customer can send a request to opt out.

All rules and regulations are only as good as the manner in which they are enforced. Let's walk through an example in a Body Corporate which has a Managing Agent, where the levy statements for one scheme get mixed up with another complex, and all unit owners receive each other's financial information. Any person involved in this ghastly exchange of information may lay a complaint against the Managing Agent and the Body Corporate with the Information Regulator. The Regulator can investigate, request a mediation, refer the matter to the Enforcement Committee, and then ultimately make the final judgement. A guilty party does have the right of appeal to the High Court, and must do so within 180 days.

Section 107 of the Act deals with penalties and administrative fees. Any person or company convicted of an offence in terms of the Act is liable to a fine or imprisonment not exceeding 10 (ten) years or R10 million, depending on which provision of the Act has been contravened.

As can be seen even very large companies who have strong firewalls and anti-virus programmes are still vulnerable to and fall victim to cyber attacks. Mike Addison from Addsure will tell you that losses include, loss of income, downtime, loss of data, and most of all loss of confidence by affected clients which could result in a huge loss of business. Managing Agents would be well advised to cover themselves with cyber liability insurance.

My view is that it is important for Managing Agents and Trustees to start taking steps to comply with the Act and to ensure that Bodies Corporate stay at the forefront of the latest laws.

Marina Constas (BA LLB FA Arb)

Director

BBM Attorneys