CGF
RESEARCH INSTITUTE
(PTY) LTD
Corporate Governance Framework®

ARTICLE

POPI: THE RIGHT TO PROTECT YOUR PERSONAL INFORMATION
26 January 2016
Johannesburg

By Terrance Mark Booysen and reviewed by Nicholas Hall (Associate: Michalsons Attorneys)

Last year there was a flurry of activity when it was reported that a well-known South African cell phone company closed its e-billing portal over an alleged security breach. Considering the potential that their customer's billing information could have become exposed, the mobile operator was quick to respond. Soon thereafter the company implemented data encryption, together with customer identification login confirmation facilities. Then there was the case of the City of Johannesburg who reportedly had massive security flaws where allegedly it was possible for non-employees to read its customer's billing information, furthermore gaining access to the customer's name, account numbers and contact details.

Whilst these incidents of potentially accessing customer privileged information is miniscule in comparison to the well-publicised and documented case of Ashley Madison, where over 30 million customer's personal and financial information was infiltrated, it does beg the question of just how safe customer's information is by those who hold this information, and of course how it is being protected against any form of abuse.

"In Canada, Ashley Madison is already facing a $578m class action lawsuit over the breach. If this breach had to happen to a South African company…heavy fines could be imposed. This is because local companies that fail to take adequate measures to protect client information on the internet could find themselves in breach of the Protection of Personal Information (Popi) Act.

Ashley Madison hack 'a lesson' for SA firms (24 August 2015)

Any organisation or persons in South Africa who capture, use and store a person's personal information, will need *that person's* consent to make use of this information. Indeed, where there is an existing relationship between the parties, then it will need to be understood -- and agreed -- by the customer as to the reasons why holding their personal information is necessary, and how their information will be used.

In the case where there is no existing relationship, for example a direct marketing company, then the company who managed to acquire the potential customer's information will only have one chance to ask that customer whether or not they would like to continue receiving their marketing communications. Should the company *not* provide the potential customer an 'opt out' option such where they choose not to receive such information, and indeed also do not wish for their personal information to be retained by the company, the individual in question will have the right to report that company to the regulator.

The Protection of Personal Information Act 4 of 2013 ('POPI') aims to regulate the processing of personal information by public and private bodies. Accordingly, organisations that process personal information will have to be aware of -- and comply with -- the provisions of POPI, and they will need to 'get their houses in order' so to speak by rapidly setting up adequate security protocols, not least also ensuring their employees adhere strictly to the process of appropriately gathering, using and securing the personal information of their existing and future customers.

PROUDLY SOUTH AFRICAN

CGF
RESEARCH INSTITUTE
(PTY) LTD
Corporate Governance Framework®

ARTICLE

Whilst many of the larger organisations may already have introduced new provisions to comply with POPI which was signed into law on 27 November 2013, smaller companies (who are equally bound to comply with this Act) may still not have made strides in this area. By failing to comply with POPI, non-compliant companies who illegally retain customer's information would also be violating that person's constitutional rights to privacy which is contained in section 14 of the Constitution of the Republic of South Africa (1996). These rights state that everyone has the right to privacy and this includes the right to be protected against the unlawful collection, retention, dissemination and use of personal information.

Whilst POPI is now a part of our statute, the actual commencement date of POPI is still to be determined by proclamation in the Government Gazette. From the date of commencement, 'responsible parties' will have one year to demonstrate their compliance with POPI. POPI defines a 'responsible party' as "a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information". This includes organisations dealing with the information of private individuals. The personal information which is protected by POPI includes information relating to the: (i) demographics (race, gender, sex, marital status, national, ethnic or social origin, colour, sexual orientation, age); (ii) contact details (e-mail address, physical address, telephone number, location); and (iii) history (education or medical, financial, criminal or employment history). Indeed if this information is not protected in the manner prescribed, then the individual could approach the Information Regulator who will ensure the appropriate sanction.

There are eight conditions that must be complied with for personal information to be processed lawfully, namely: (i) accountability; (ii) processing limitation; (iii) purpose specification; (iv) further processing limitation; (v) information quality; (vi) openness; (vii) security safeguards; and (viii) data subject participation. There are, however, certain exclusions and exemptions from having to comply with these conditions that organisations should be aware of. Failure to comply with POPI may cause serious damage to an organisation. Not only may it result in reputational damage, but anyone found guilty of an offence in terms of POPI may be liable to imprisonment of up to ten (10) years or a fine of up to R10 million.

As there are many negative actions which could result where personal information has been violated or negligently disclosed -- and this includes the perils associated with identity theft -- POPI has come at a time when there is a heightened awareness surrounding our personal rights and personal safety. Indeed as technological and social media advances have made great strides in many areas, so too have there been negative connotations. Accordingly, whilst there are a number of changes organisations will need to adopt and systems which will need to be implemented, many people are pleased with the introduction of POPI which was modelled off the well-honed European Union legislation for protecting personal information.

"Global risk reports are citing cyber as one of the top 10 risks companies should be considering, but in South Africa, specialist cyber insurance is a new concept to most…

This may be because many enterprises do not know the real value of the data they manage, and find it difficult to predict the potential losses they could suffer in the event of a hack, denial of service attack or data being lost…"

SA enterprise unprepared for breaches (27 March 2014)

PROUDLY SOUTH AFRICAN

CGF
RESEARCH INSTITUTE
(PTY) LTD
Corporate Governance Framework®

ARTICLE

There is no doubt that South African organisations -- as well as other 'responsible parties' -- will need to take this piece of legislation very seriously, especially in light of the fact that our society has never really been one to take privacy that seriously. Due to the broadness of this Act, and considering for example the many people in a retail store who deal with customer's personal information on a daily basis, each employee will need to be on top of this legislation to ensure they are all protecting the customer's information. Indeed the variables are vast, and just one error from any one of the employees could result in disaster for both the employee and the organisation.

As this Act begins to take effect, expectedly organisations will need to take greater precautions as they get rid of old office records containing personalised customer information, or when their office security guard insist on you completing all your personal information on their building entrance forms. Hopefully we will also see the end of those marketing companies who harass people with their annoying unsolicited phone calls and endless email spam.

ENDS

Words: 1,326

For further information contact:

CGF Research Institute (Pty) Ltd
Terry Booysen (Chief Executive Officer)
Tel: 011 476 8264
Cell: 082 373 2249
E-mail: tbooysen@cgf.co.za
Web: www.cgf.co.za

Michalsons Attorneys
Nicholas Hall (Associate)
Tel: 086 011 1245
Cell: 082 675 33 72
E-mail: nicholas@michalsons.co.za
Web: www.michalsons.co.za

About CGF Research Institute (Pty) Ltd: Services

CGF is a Proudly South African, Level 4 B-BBEE complaint company that specialises in conducting desktop research on Governance, Risk and Compliance (GRC) related topics, amongst other related company secretariat, regulatory and compliance services.

The company has developed numerous products that cover GRC reports designed to create a high-level awareness and understanding of issues impacting a CEO through to all employees of the organisation.

Through CGF's Lead Independent Consultants, our capabilities include the aggregation of local and international best of breed governance reporting services and extend to;

- strategic management consulting, business re-structuring, executive placements, executive coaching, board assessments and evaluation, out-sourced company secretarial functions, facilitation of Corporate Governance Awareness workshops, IT governance through to Enterprise Risk Management (ERM) consulting and Corporate Reputation services.

All CGF's services cater for large corporates, small and medium sized businesses and state owned organisations. To find out more about CGF, its Lead Independent Consultants and Patrons access www.cgf.co.za or www.corporate-governance.co.za

PROUDLY SOUTH AFRICAN