ARTICLE

THE PROTECTION OF PERSONAL INFORMATION ACT IS LAW: WHERE TO FROM HERE?
Johannesburg
16 May 2014

Article by Dr Peter Tobin, John Cato and Professor David Taylor

Do you remember the old story about how to get things moving? That's right, the one about the stick and the carrot! Well now we have something new to focus our attention on, namely the Protection of Personal Information Act No.4 of 2013 ('POPI'). POPI was gazetted in late 2013, with partial commencement in April 2014; indeed now is the time to get things moving in terms of compliance with this important Act.

So where is the "stick and carrot" for POPI?

Think about how broad the definition of "personal information" can be: customers, employees, suppliers, in fact anyone we interact with as a business. The POPI Act was signed into law in November 2013 and is expected to become effective in the next few months. Organisations will then have twelve months to become fully compliant or face the prospect of some potentially stiff penalties (including fines of up to R10 million) or worse reputational damage and loss of customers. That's the "stick" part of the deal.

The "carrot" aspect is the opportunity to boost confidence in your business by demonstrating the way you manage sensitive personal data. Personal information includes data of customers, suppliers and employees, whether they are in emails, invoices, databases or printouts. This means showing you have processes and procedures in place to handle effectively and securely all aspects of what's covered in the POPI Act.

Where does POPI come from?

Privacy and Data Protection Acts have already existed in other countries for several years. Examples of these are the European Union (EU) Data Protection Act which came into effect in 1995, the UK Data Protection Act (1998). The POPI Act is modelled on the EU legislation to a large extent, and POPI has been written to ensure that South Africa is line with international best practice.

Conditions for lawful processing of personal information in the POPI Act

- ***Accountability** = assigning ownership in your business;*
- ***Processing limitation** = processing information for lawful reasons and in a manner that does not infringe privacy;*
- ***Purpose specification** = only obtaining and holding personal information for a specific purpose;*
- ***Further processing limitation** = further processing of personal information must be compatible with the purpose for which it was collected;*
- ***Information quality** = ensuring that information is complete and accurate;*
- ***Openness** = informing individuals that their information has been obtained and the purpose thereof;*
- ***Security safeguards** = the integrity of personal information must be secured using reasonable technical and organisational measures;*
- ***Data subject participation** = an individual has the right to request whether an organisation holds their personal information. An individual may request the information is deleted or corrected if it is incorrectly stored.*

What does POPI mean to you and your stakeholders?

- Personal information such as employee and customer information will have to be protected and processed in a different way, in accordance with the conditions of the Act;
- Employee and customer information may not be disclosed to another party without the person's consent;
- Employee and customer information will have to be destroyed in a controlled manner when the purpose for which the information is held is no longer valid;
- Standards will have to be defined for shredding equipment -- similar to standards in other countries -- so that the Act can be applied to in an appropriate manner;
- Steps should be taken to ensure that personal information stored on removable media such as memory sticks is protected in a controlled manner and consideration should be given to providing advice to consumers in the area.

POPI "Dos and Don'ts"

Do:

- Understand what the POPI Act means to your business
- Make sure you have assigned ownership for compliance with POPI
- Start by conducting an assessment of how far you are already compliant
- Develop a plan to address areas of non-compliance identified
- Engage with all the relevant stakeholders impacted by POPI
- Remember the "stick and carrot" aspects of POPI
- Think about the implications of POPI for the products and services you provide

Don't:

- Ignore POPI, it won't go away!
- Put off your compliance efforts just because you have a twelve month grace period
- Underestimate the amount of work that is required to change your business policies, processes and procedures, documentation and systems
- Panic! POPI compliance is more like climbing Table Mountain than Mount Everest
- Rush into your compliance efforts; take a structured, project-based approach to make your compliance efforts effective

So where should you start?

A number of steps should be taken to prepare for POPI becoming effective. These include:

- Organisational – start a POPI preparation programme and appoint an Information Officer to drive your POPI compliance initiatives. An awareness and training programme should be prepared and delivered so that everyone in the business understands the implications of POPI;
- Legal – review contracts with service providers where personal information is stored on your company's behalf. For example, if you have outsourcing arrangements in place, ensure that these are amended to include personal information protection. This applies to business partners as well, where customer information is shared with them;
- Business – identify processes where personal information is involved. Examples include customer and supplier information, including the handling of employee information. These processes should be amended to ensure that they comply with the principles in the POPI Act;
- Technology – electronically stored personal information should be identified and steps taken to ensure that such information is protected in line with the Security safeguards principle contained in the Act.

Ends

Words: 652

For further information contact petert@iact-africa.com or johnc@iact-africa.com
Further information about CGF can be found at www.cgf.co.za

Contact details:

CGF Research Institute (Pty) Ltd
Terry Booysen (Chief Executive Officer)
Tel: +27 (0) 11 476 8264
Cell: +27 (0) 82 373 2249
E-mail: tbooysen@cgf.co.za

IACT Africa
Dr. Peter Tobin (Consultant)
Tel: +27 (0) 10 500 1038
Cell: +27 (0) 83 922 3444
E-mail: petert@iact-africa.com

About IACT Africa

IACT Africa is a specialist business consulting company with a focus on assisting organisations to add strategic value to IT Governance and IT Management. Programmes and projects in the IT Governance and Management area are often initiated for compliance reasons and are not viewed from potential business benefit perspectives.

IACT Africa offer consulting services in Africa as well as a number of online resources that can help you to carry out governance projects wherever you are located without the need for consultants. We are also able to recommend world class IT GRC software.

About CGF Research Institute

CGF is a Proudly South African company that specialises in conducting desktop research on Governance, Risk and Compliance ('GRC') related topics. The company has numerous products and professional consulting services that cover; GRC reporting, board evaluation assessment and induction, mentoring and coaching, executive search and Non-Executive director placements, group wellness, including the compilation of Integrated Reports and verification.