THE PROTECTION OF PERSONAL INFORMATION BILL: A 20 MINUTE OVERVIEW

Category: Commercial Law,Privacy Law, Infosec, and POPIA
written by Lucien Pierce | October 25, 2013

1. The Protection of Personal Information Bill ("POPI") in context

1.1. Why do we need POPI and how does it affect your organisation?

1.1.1. We need it because the right to privacy is one of the pillars of South Africa's Bill of Rights. This right to privacy must be balanced with the right to access to, and the free flow of, information.

1.1.2. Processing information is an integral part of many businesses and has become even more important in the information age. Whilst certain best practices and procedures for protecting personal information may already have been implemented in some better run organisations, these have never had the force of law.

1.1.3. Once POPI is promulgated, the protection of personal information will be regulated by law. Failures to comply will expose many organisations to investigation and major sanctions.

1.1.4. You effectively have one year from the date that POPI is passed into law, to put practices and procedures in place that ensure compliance with POPI.

1.1.5. Is your organisation included in the 41% of organisations that have yet to begin planning and implementing POPI compliance processes and procedures?

1.2. An overview of POPI's provisions

1.2.1. POPI essentially regulates what we do with personal information once we receive and process it.

1.2.2. It seeks to make us accountable for what we do with personal information. It ensures that we only process information in a limited way and for very specific purposes.

1.2.3. It seeks to prevent our personal information from being processed or used further than what it was originally given for. It allows us to check that the quality of the information that people have is correct and allows us to be entitled to ask what information is held on us.

1.2.4. Importantly, it places an obligation on data processors to ensure that our personal information is safe and is secured in the most appropriate way. It allows us to participate in what is done with our personal information and how it is used.

1.3. What other legislation, regulations and policies does POPI relate to?

1.3.1. POPI does not operate in isolation. It is complemented by the Promotion of Access to Information Act.

1.3.2. POPI's objectives are also complemented by a number of sector specific Acts, regulations and

best practices. For example, the Companies Act makes provision for the protection of information.

1.3.3. In a similar way, as much as POPI deals with the methods of securing information, the King III Code recommends measures and standards that should be followed to secure information.

2. Some important definitions to consider

2.1. POPI protects the personal information of "data subjects". A data subject is a person to whom personal information relates. It includes legal entities e.g. companies.

2.2. What is an "information officer"? This is defined in the Promotion of Access to Information Act, but basically refers to the head of the particular organisation.

2.3. What is "personal information"? This is information relating to an identifiable, living, natural person and may also apply to legal entities. It includes a wide range of information including race, gender, physical or mental health, biometric information and even personal opinions.

2.4. POPI regulates "processing" of information by anyone regarded as a "responsible party"? Processing is defined very widely, but in essence means any operation or activity concerning personal information. You are a responsible party if you are a body which on your own or with others, determines the purpose and means for processing personal information.

2.5. What are "records"? A record is any recorded information in any form or medium which is in a responsible party's possession.

3. Does POPI apply to everyone? In what circumstances would you or your organisation be exempt from POPI's provisions?

3.1. What about personal information you use at home, what if there is a crime taking place and personal information needs to be disclosed, what if it is required for purposes of national security, what about journalists who want to write about celebrities or politicians?

3.2. POPI considers these situations and acknowledges that there have to be some exemptions or else absurd situations would arise. It provides exemptions in the situations listed above.

4. The 8 principles: practical examples demonstrating what conditions ensure lawful processing of personal information

4.1. Accountability

4.1.1 Responsible parties need to ensure that they are accountable.

4.1.2. What does this mean in practical terms? It means that your organisation needs to be aware of POPI and what its requirements are.

4.1.3 In essence, your organisation will be held accountable for any non-compliance with POPI.

4.2. Processing limitation

4.2.1. The days of freely sharing information and transferring them between organisations are gone.

4.2.2. You may only process information lawfully. POPI goes into detail and explains what lawful processing is.

4.2.3. You may not process personal information excessively. It should only be processed for reasons which are adequate and relevant.

4.2.4. You may only process information if you have consent, if it is justified, if you collected it directly from the person and the person is entitled to object to such processing.

4.3. Purpose specification

4.3.1. The information that your organisation collects from people must be used for a specific purpose. So collecting information for one reason and then use it for another may contravene POPI.

4.3.2. Information that is collected should only be kept for as long as is reasonably necessary. POPI deals with this in detail.

4.4 Further processing limitation

4.4.1 Very much like the purpose specification further processing of personal information should only occur if it is in line with the original purpose for which it was collected.

4.5. Information quality

4.5.1. Your organisation is required to take reasonable steps to ensure that personal information that is held, is up-to-date. This means updating it where necessary.

4.6. Openness

4.6.1. Data processors must have a record, as required by the Promotion of Access to Information Act, of all processing operations for which they are responsible.

4.6.2. An organisation collecting personal information should generally notify people in advance, that it is collecting information on them. It should advise them of what the information will be used for, what information will be collected, how the information will be stored and for how long. Think of the CCTV cameras in on your organisation’s premises. Do you think that these fall under POPI’s provisions? If so, how would POPI impact on the use of the CCTV cameras?

4.7. Security safeguards

4.7.1 POPI places great weight on the security, integrity and confidentiality of personal information. What “appropriate, reasonable, technical and organisational measures” is your organisation taking, because this is what POPI requires? How much is expected of your organisation: should you have cutting edge measures or will very basic measures suffice?

4.7.2. POPI addresses situations where the processing of personal information is outsourced to a third party? It places certain security obligations on the processing of such information and requires that these also apply to the third parties you use.

4.7.3. Have you got a data breach crisis management plan in place? You may ask why, but there are

obligations to report data breaches to the Information Regulator, determine what data has been lost and notify the people whose data has been breached.

4.8. Data subject participation

4.8.1. A data subject has the right to check whether you hold any personal information on him or her. If the information you hold is incorrect, the data subject has the right to require you to correct it.

4.9. Processing of special personal information or personal information of children

4.9.1. POPI prohibits the processing of special personal information (such as religious or philosophical beliefs, race, health or biometric information) or information of children.

4.9.2. It does however provide certain exemptions, which permit the processing of such information in very limited circumstances. For example, a church or a mosque would be able to process the personal information of its members.

5. Supervision: the Information Regulator and how it will operate

5.1. The Information Regulator is a legal entity that will be formed to provide education, monitor and enforce compliance, consult with interested parties, handle complaints, conduct research, issue codes of conduct and perform other related activities provided for in POPI.

6. Prior authorisation to process personal information and consequences of not complying

6.1. There is an obligation to register as a responsible party, if you process information. This registration must be made with the Information Regulator and must happen before personal information is processed.

7. Codes of conduct: what they are and why they can simplify matters for groupings in your organisation

7.1. POPI recognises that it would be a mammoth task for the Information Regulator to police every complaint.

7.2. It therefore contemplates codes of conduct for different industries and groupings, such as public sector organisations that operate in a particular industry e.g. telecommunications or health.

7.3. They can subscribe to such codes of conduct and effectively be part of a self-regulating industry.

8. Data subjects’ rights regarding direct marketing, unsolicited communications and automatic

decisions: public sector considerations

8.1. POPI regulates unsolicited communications and the parameters within which organisations may market to people. It essentially provides that direct marketing may only take place in circumstances where the marketer has obtained the data subject's consent.

9. Trans-border information flows and public sector considerations

9.1 POPI prohibits the transfer of personal information to third parties in foreign countries, except in certain circumstances. Transfers that may be permitted include where the foreign country has a law, binding corporate rules or binding agreements that provide an adequate level of protection similar to what is contained in POPI.

10. Enforcement: an overview of the practical aspects of POPI's enforcement

10.1. POPI sets out how the Information Regulator will deal with complaints regarding contraventions of POPI. It deals with how complaints could be settled or investigated and rulings enforced.

11. Offences, penalties and administrative fines

11.1. POPI provides for fines of up to R10 million and / or imprisonment for up to 10 years.