Revealing privacy in South Africa:
What you need to know

By Information Security Group Africa: Privacy Special Interest Group

September 2011
Table of Contents

1. Acknowledgements .................................................................................................................... 6

2. Introduction ............................................................................................................................... 9
   2.1. Privacy – What is it? ............................................................................................................. 9
   2.2. Why is information privacy important? ............................................................................... 9
   2.3. The context of privacy legislation .......................................................................................11
   2.4. Concepts relevant to privacy ..............................................................................................11

3. The current legislative landscape affecting privacy ................................................................. 14

4. The Protection of Personal Information Bill [B2 ... 2009] (PoPI) ............................................... 25
   4.1. Introduction ........................................................................................................................25
   4.2. Overview of the Protection of Personal Information Bill [B2 ... 2009] (PoPI) ....................26
   4.3. Personally Identifiable Information (PII) ............................................................................27
   4.4. The impact of PoPI on the Public Sector ...........................................................................30

5. An overview of the privacy principles ....................................................................................... 33

6. Establishing an information protection culture ........................................................................ 38
   6.1. What is an information protection culture? ........................................................................38
   6.2. The impact of PoPI on an information protection culture ..................................................38
   6.3. Implementing an information protection culture ...............................................................39
   6.4. Measuring an information protection culture ....................................................................39

7. The impact of PoPI on different industries ............................................................................... 42
   7.1. Financial and insurance sector ...........................................................................................42
   7.2. Health care sector ..............................................................................................................43
   7.3. The Information, Communications and Technology (ICT) Industry ..................................47
   7.4. The South African public sector .........................................................................................49

8. PoPI and Trans Border Personal Information Flows .................................................................. 53

9. The business units that will be affected most ........................................................................... 56
   9.1. Legal and Regulatory ........................................................................................................56
   9.2. Governance, Risk and Compliance ...................................................................................56
   9.3. Information Technology ....................................................................................................56
   9.4. Human Resources Development and Training ..................................................................57
   9.5. Procurement Services / Vendor- and Third-Party Management .........................................57
   9.6. Marketing ...........................................................................................................................57
   9.7. Product and Service Development ....................................................................................58

10. The people, process and technology considerations when implementing privacy requirements 60
    10.1. People components ............................................................................................................61
    10.2. Process components ........................................................................................................63
    10.3. Technology components ..................................................................................................70

11. The price of non-conformance .................................................................................................. 77
List of Figures

Figure 1: The scope and applicability of PoPI .............................................................................................................. 29
Figure 2: The exclusions of PoPI .................................................................................................................................. 30
Figure 3: Flow of data to support patient care in the health environment................................................................. 44
Figure 4: People components......................................................................................................................................... 61
Figure 5: Governance process ....................................................................................................................................... 64
Figure 6: Technology component considerations...................................................................................................... 72
Figure 7: Verizon report – Breaches [8] ......................................................................................................................... 75

List of Tables
Table 1: Current legislative landscape ........................................................................................................................ 14
Table 2: Other Acts that impact on the processing of personal information .............................................................. 23
Table 3: Summary of the eight privacy principles ....................................................................................................... 33
Table 4: Overview of health care legislation ................................................................................................................ 45
Table 5: Privacy frameworks and standards................................................................................................................ 60
Table 6: Privacy and information security awareness days .......................................................................................... 62
Table 7: Process components – Governance and plan................................................................................................. 64
Table 8: Process components – Define and Implement ............................................................................................... 65
Table 9: Process components - Verify ......................................................................................................................... 70
Table 10: Process components – Act ............................................................................................................................ 70
Table 11: Technical Controls........................................................................................................................................... 73
Table 12: Privacy Enhancing Technology (PET)........................................................................................................... 73
Table 13: Privacy drivers.................................................................................................................................................. 77
Table 14: Data breaches/incident in South Africa ......................................................................................................... 79
1. Acknowledgements

The preparation of this document was conducted by the Privacy Special Interest Group of the Information Security Group Africa. The following bodies provided input to the document.

Aptronics Pty (Ltd) - Peet Smith
Business Connexion Group Limited - Julius Francis
Candor Governance Specialists - Carolynn Chalmers
Chetty Law - Pria Chetty
Critical Identity - Iain Campbell
Deloitte & Touché - Natalie Naicker
Government Employees Pension Fund - Karien Lombard
Information Security and Privacy Consultant - Paul Strauss
KPMG Services (Proprietary) Limited - Farzana Badat
Legate ICT Consulting - Helaine Leggat
Liberty Group Limited - Oscar Stark
MTN Pty (Ltd) Group - Candice Govender
Organisational Diagnostics CC - Dr. Adéle da Veiga
Sanlam - Brian Abdoll
UTi Worldwide Inc. - Daniel de Jager
Vodacom Group Limited - Tamina Hari, Emile Swanson
Webber Wentzel - Pierre Liddle

Edited by:
Dr. Adéle da Veiga and Tamina Hari

Legal Review by:
Deloitte & Touché – Risk Advisory, Dean Chivers

Input to Legal Review:
Legate ICT Consulting, Helaine Leggat

Graphical Layout and Formatting by:
Deloitte and Touché – Risk Advisory

On behalf of the ISG Africa Privacy Special Interest Group a sincere thank you to all the above parties for their time, knowledge contributions and input to produce this document. We would also like to express thanks to members who participated in the SIG meetings and contributed in the discussions.
About ISG Africa

ISG Africa is a non-profit organisation founded in 2005 and created in response to the increase of information security threats facing organisations and public sector in Africa. This volunteer Group consists of security professionals from the public and private sectors across Africa. ISG Africa’s aim is to provide the mechanism for regular exchange of information security knowledge and facilitate networking between members and the stakeholder community, whilst raising awareness of information security vulnerabilities and global threats in the context of Africa.

Members of the Privacy Special Interest Group (SIG) benefit from sharing privacy knowledge and practical solutions drawn from the considerable experience within their organisations and developed through our networking and interaction programme.

For further information about the Privacy Special Interest Group please contact:

Dr. Adele da Veiga, adele.daveiga@vodamail.co.za

Caveat

This document has been compiled with care by the ISG Africa Privacy Special Interest Group to the best of the ability of the individual contributors and ISG Africa as a whole. The purpose of this document is to provide general information only and is in no way to be construed as the provision of legal or professional advice. The ISG Africa and the individual contributors accept no liability whatsoever or howsoever arising from any reliance on the contents of this document.
Introduction
2. Introduction

2.1. Privacy – What is it?

The Oxford Dictionary defines “privacy”, as “the state of being left alone and not watched or disturbed by other people”. From a business perspective it means that personal information must be used in an appropriate manner within defined parameters. The appropriateness of the use of personal information depends on a number of factors such as context, regulatory requirements, the individual’s expectations as well as the right of an individual to control how their personal information is used or ‘processed’.

There are different types of privacy that individuals have rights to, each emphasising different aspects of privacy. These include:

- physical privacy - relevant to government search and seizure operations and peeping toms;
- bodily and decisional privacy - concerned with choice and the integrity of an individual’s body, the right to abortion and cavity searches;
- proprietary privacy - concerned with publicity, media representation and celebrity, ownership and control of the body, appearance and identity; and
- information privacy - the interest an individual has in controlling information about them.

It is important to understand that organisations have certain obligations when processing personal information and that individuals have certain rights. These may be established in laws, regulations and organisational policies. South Africa’s Protection of Personal Information Bill [No. 9 of 2009] (PoPI) is primarily focused on ‘information privacy’, also known as ‘data protection’ or ‘data privacy’.

This document provides an overview of the principles encapsulated in PoPI focusing on its impact across all sectors and some specific industries.

2.2. Why is information privacy important?

With globalisation, countries, economies and businesses have been able to reach greater and more diverse markets. This means that people and businesses in various countries with different jurisdictions and countless legal differences all participate in processing personal information that is valuable and that requires protection.

Globally, an increasing number of foreign laws are aimed at protecting individuals and preserving and strengthening human rights. Many countries have promulgated laws that explicitly address the protection of personal information. It makes sense, that because of the different jurisdictions, cultures and histories of countries, these laws are different.

Globalisation and economic imperatives have driven the need for cooperation, and over time, certain fundamental principles have arisen. Privacy is viewed as a fundamental human right and the cornerstone of a democratic society. It lies at the foundation of customer-client confidentiality and the value society places on the autonomy of the individual. The ability to maintain privacy is also viewed as one of the main enablers of electronic commerce.

Internationally, countries have recognised the requirement to ensure that the right of individuals and that of society should be protected. This is not only required to maintain the rights of society, but support the underlying trust which drives relational interaction on both a local and international level, enabling commerce. This need has fuelled a global drive, for the regulation of privacy.
Privacy in other countries

In Europe, modern privacy legislation has been maturing since 1981, with the establishment of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, as a European Council negotiated directive. This foundation piece was later built upon by the establishment of the 1995 Data Protection Directive. This addition was necessitated by the free flow of personal information in the context of a globalising economy driven by technical advances.

In the United States the approach which drove the establishment of privacy legislation followed a more disparate path. The foundation of commerce in the United States is based on the laissez-faire principle (a free flowing private transactional engagement, without state intervention) and as such, the various states regulate themselves independently.

Canada has very strict privacy laws, namely The Personal Information Protection and Electronic Documents Act as well as the Privacy Act. Many other counties also have privacy regulations for instance Hong Kong, Japan, Australia and New Zealand.

Refer to www.informationshield.com/intprivacylaws.html for international privacy laws by country. Another useful site is www.mofo.com/privacylibrary

Privacy in South Africa

In the South African post apartheid context the value of privacy is appreciated. This post apartheid backdrop created the foundation for privacy which is articulated in the Constitution and the Bill of Rights. In an effort to solidify South Africa as a global economic player, the legislative underpinnings echoed in the Protection of Personal Information Bill are required to enable global commerce and cross jurisdictional information flow. This underlying trust enabler will not only protect the exchange of personal data in the South African environment, but align South Africa to international standards, thereby empowering South Africa and organisations in commercial relations.

Globally, trade has inflicted the lobbying for controls which regulate and maintain the economic underpinnings without transgressing material rights of individuals. Privacy legislation also provides a platform to help drive electronic commerce.

The value of privacy legislation may also become evident in its application. The global economy considers cost leveraging as an opportunity. In this spirit, many companies utilise mechanisms such as outsourcing transactional processing to establish cost competitive advantages in foreign countries. Cross-border flow of data, which often includes personal information, necessitates control to maintain the underlying commercial value, but also the protection of such data. For this reason many countries have regulated outsourcing practises.

The imminent legislation may be embraced by some businesses as an opportunity to attract and retain business.

The Bill of Rights entrenched the rights of individuals.

The Protection of Personal Information Bill addresses how the privacy of an individual's personal information may be protected.
2.3. The context of privacy legislation

In order to understand and appreciate the boundaries of the right of privacy and to balance privacy with other competing rights in the Constitution of South Africa, 1996, it is important to place privacy in the economic and political context in which personal information is used.

There is considerable monetary value attached to personal information. Criminal elements are enticed by the financial value of dealing in and trading with personal information. Personal information is invaluable. ‘Identity theft’, a form of fraud, occurs when someone pretends to be someone else by assuming that person’s identity. This is typically done in order to access resources or obtain credit and other benefits attached to that person’s name. The victim of identity theft, meaning the person whose identity has been assumed by the identity thief, can suffer adverse consequences if held accountable for the perpetrator’s actions, has funds stolen or has their identity sold to criminal organisations.

There are numerous legitimate reasons for the use for personal information both nationally and internationally. In order to contextualise privacy, the following are relevant considerations:

- the fight against terrorism;
- crime in a global economy across different jurisdictions, requiring cooperation for effective enforcement;
- government necessity in collecting personal information, administrative necessity such as birth, death and marriage records and the issuance of identity documents, passports and visas;
- public health reporting and protection against epidemics;
- administrative necessity, such as census statistics information required for business necessity such as information required for tenders or profiling; and
- the media’s interest in personal information and the interest of the public.

2.4. Concepts relevant to privacy

Confidentiality

Confidentiality ensures that information is accessible only to those who are authorised to access it. It means that information must be protected throughout its life cycle in any form, while in storage, processing or transport.

Personal information is not necessarily confidential, for example, a person’s gender may be well known, home address and landline contact information may be published in a telephone directory.

Information security

Information security deals with the securing of the confidentiality, integrity and availability of information. An example of information security practice is restricting the access of information to authorised persons. The confidentiality of information may be improved through the implementation of security controls. Appropriate information security measures and techniques are vital to securing the confidentiality of the protected information. It is impossible to ensure the confidentiality of information that was not initially classified “confidential”.
**Information security and privacy**

The purpose of security is to provide mechanisms that are intended to limit the vulnerability of assets and resources. There are several kinds of security. Some of them are:

- physical security - relevant to the securing of buildings and factories from incidents of theft or fire;
- national security - concerned with the protection of a country, including the identity of its citizens and information critical to the safety and security of the state; and
- information security - relates to the protection of information or data. It encompasses, amongst others, techniques for ensuring that data stored in computers and data travelling across telecommunication networks, cannot be intercepted or read by unauthorised persons or be compromised in any way.

Information security aims to protect the confidentiality, integrity and availability of information and information systems.

Privacy, specifically data privacy, concerns the control individuals have over information relating to themselves. The control may be exercised in a number of ways, for example, by granting individuals the right to know when information is collected, the right to decide whether this information may be used, for what purposes and by whom.

It is accepted that adequate security measures are necessary to protect the privacy of personal information. Security of personal information is an essential part of protection of privacy rights. Privacy cannot exist without securing the personal data. Information security is an integral component of privacy. A number of these concepts have been incorporated into South Africa’s proposed privacy legislation.
The Current Legislative Landscape Affecting Privacy
3. The current legislative landscape affecting privacy

There is no single piece of existing legislation that addresses privacy to date. Referenced below, in table 1, is a summary of legislation that contains privacy related sections.

Table 1: Current legislative landscape

<table>
<thead>
<tr>
<th>Legislation</th>
<th>Summary of provision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constitution Act 108 Of 1996</td>
<td></td>
</tr>
<tr>
<td><strong>Section 14</strong> (Privacy)</td>
<td>Everyone has the right to privacy, which includes the right not to have:</td>
</tr>
<tr>
<td></td>
<td>- their person or home searched; their property searched; their possessions seized; or</td>
</tr>
<tr>
<td></td>
<td>- the privacy of their communications infringed.</td>
</tr>
<tr>
<td><strong>Section 32</strong> (Access to Information)</td>
<td>- Everyone has the right of access to any information held by the state;</td>
</tr>
<tr>
<td></td>
<td>- and any information that is held by another person that is required for the exercise or protection of any rights.</td>
</tr>
<tr>
<td><strong>Section 36</strong> (Limitation of Rights)</td>
<td>The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including:</td>
</tr>
<tr>
<td></td>
<td>- the nature of the right;</td>
</tr>
<tr>
<td></td>
<td>- the importance of the purpose of the limitation;</td>
</tr>
<tr>
<td></td>
<td>- the nature and extent of the limitation;</td>
</tr>
<tr>
<td></td>
<td>- the relation between the limitation and its purpose; and</td>
</tr>
<tr>
<td></td>
<td>- less restrictive means to achieve the purpose.</td>
</tr>
<tr>
<td>Promotion of Access to Information Act 2 of 2000</td>
<td>&quot;private body&quot; means—</td>
</tr>
<tr>
<td>Definitions</td>
<td>- a natural person who carries or has carried on any trade, business or profession, but only in such capacity;</td>
</tr>
<tr>
<td></td>
<td>- a partnership which carries or has carried on any trade, business or profession; or any former or existing juristic person.</td>
</tr>
<tr>
<td></td>
<td>&quot;personal information&quot; means information about an identifiable individual, including, but not limited to:—</td>
</tr>
<tr>
<td></td>
<td>- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;</td>
</tr>
<tr>
<td></td>
<td>- information relating to the education or the medical, criminal or employment history of the individual or information relating to financial</td>
</tr>
<tr>
<td>Legislation</td>
<td>Summary of provision</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Legislation</td>
<td></td>
</tr>
</tbody>
</table>
| transactions in which the individual has been involved; any identifying number, symbol or other particular assigned to the individual; the address, fingerprints or blood type of the individual;  
  • the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;  
  • correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;  
  • the views or opinions of another individual about the individual;  
  • the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and  
  • the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but excludes information about an individual who has been dead for more than 20 years. |
| Section 4 (Records held by official or independent contractor of public or private body) | For the purposes of this Act, but subject to section 12 [public bodies and officials], a record in the possession or under the control of—  
  • an official of a public body or private body in his or her capacity as such; or  
  • an independent contractor engaged by a public body or private body in the capacity as such contractor, is regarded as being a record of that public body or private body, respectively. |
| Section 9 (Objects of the Act)                                           | The objects of this Act are— to give effect to the constitutional right of access to—  
  any information held by the State; and any information that is held by another person and that is required for the exercise or protection of any rights; to give effect to that right—  
  subject to justifiable limitations, including, but not limited to, limitations aimed at the reasonable protection of privacy, commercial confidentiality and effective, efficient and good governance. |
| Section 63 (1) and (2) (Mandatory Protection of Privacy of Third Party – Natural Person) | (1) Subject to subsection (2), the head of a private body must refuse a request for access to a record of the body if its disclosure would involve the unreasonable disclosure of personal information about a third party, including a deceased individual.  
  (2) A record may not be refused in terms of subsection (1) insofar as it consists of information— about an individual who has consented in terms of section 72 or otherwise in writing to its disclosure to the requester concerned; already publicly available;  
  that was given to the private body by the individual to whom it relates and the individual was informed by or on behalf of the private body, before it is given, that the information belongs to a class of information that would or might be made available to the public;  
  about an individual’s physical or mental health, or well-being, who is under the care of the requester and who is— under the age of 18 years; or  
  incapable of understanding the nature of the request, and if giving access would be in the individual’s best interests; about an individual who is deceased and the requester is—  
  (i) the individual’s next of kin; or  
  (ii) making the request with the written consent of the individual’s next of kin; or  
  about an individual who is or was an official of a private body and which relates to the position or functions of the individual, including, but not |
<table>
<thead>
<tr>
<th>Legislation</th>
<th>Summary of provision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legislation</td>
<td>limited to—the fact that the individual is or was an official of that private body; the title, work address, work phone number and other similar particulars of the individual; the classification, salary scale or remuneration and responsibilities of the position held or services performed by the individual; and the name of the individual on a record prepared by the individual in the course of employment.</td>
</tr>
</tbody>
</table>
| Section 64  | (1) Subject to subsection (2), the head of a private body must refuse a request for access to a record of the body if the record contains—  
  a) trade secrets of a third party;  
  b) financial, commercial, scientific or technical information, other than trade secrets, of a third party, the disclosure of which would be likely to cause harm to the commercial or financial interests of that third party; or  
  c) information supplied in confidence by a third party, the disclosure of which could reasonably be expected—  
    (i) to put that third party at a disadvantage in contractual or other negotiations; or  
    (ii) to prejudice that third party in commercial competition.  
  (2) A record may not be refused in terms of subsection (1) insofar as it consists of information about—  
    a) a third party who has consented in terms of section 72 or otherwise in writing to its disclosure to the requester concerned;  
    b) the results of any product or environmental testing or other investigation supplied by, carried out by or on behalf of a third party and its disclosure would reveal a serious public safety or environmental risk. |
| Section 65  | The head of a private body must refuse a request for access to a record of the body if its disclosure would constitute an action for breach of a duty of confidence owed to a third party in terms of an agreement. |
| Section 66  | The head of a private body—  
  must refuse a request for access to a record of the body if its disclosure could reasonably be expected to endanger the life or physical safety of an individual; or  
  may refuse a request for access to a record of the body if its disclosure would be likely to prejudice or impair—  
    (i) the security of—  
      (aa) a building, structure or system, including, but not limited to, a computer or communication system;  
      (bb) a means of transport; or  
      (cc) any other property; or  
    (ii) methods, systems, plans or procedures for the protection of—  
      (aa) an individual in accordance with a witness protection scheme;  
      (bb) the safety of the public, or any part of the public; or  
      (cc) the security of property contemplated in subparagraph (i)(aa), (bb) |
<table>
<thead>
<tr>
<th>Legislation</th>
<th>Summary of provision</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section 67</strong></td>
<td>The head of a private body must refuse a request for access to a record of the body if the record is privileged from production in legal proceedings unless the person entitled to the privilege has waived the privilege.</td>
</tr>
<tr>
<td><strong>Section 68</strong></td>
<td>(1) Subject to subsection (2), the head of a private body may refuse a request for access to a record of the body if the record—</td>
</tr>
<tr>
<td></td>
<td>• contains trade secrets of the private body;</td>
</tr>
<tr>
<td></td>
<td>• contains financial, commercial, scientific or technical information, other than trade secrets, of the private body, the disclosure of which would be likely to cause harm to the commercial or financial interests of the body;</td>
</tr>
<tr>
<td></td>
<td>• contains information, the disclosure of which could reasonably be expected—</td>
</tr>
<tr>
<td></td>
<td>• to put the private body at a disadvantage in contractual or other negotiations; or</td>
</tr>
<tr>
<td></td>
<td>• to prejudice the body in commercial competition; or</td>
</tr>
<tr>
<td></td>
<td>• is a computer program, as defined in section 1(1) of the Copyright Act, 1978 (Act No. 98 of 1978), owned by the private body, except insofar as it is required to give access to a record to which access is granted in terms of this Act.</td>
</tr>
<tr>
<td><strong>Section 69</strong></td>
<td>The head of a private body must refuse a request for access to a record of the body if the record contains information about research being or to be carried out by or on behalf of a third party, the disclosure of which would be likely to expose—</td>
</tr>
<tr>
<td></td>
<td>• the third party;</td>
</tr>
<tr>
<td></td>
<td>• a person that is or will be carrying out the research on behalf of the third party; or</td>
</tr>
<tr>
<td></td>
<td>• the subject matter of the research, serious disadvantage.</td>
</tr>
<tr>
<td></td>
<td>The head of a private body may refuse a request for access to a record of the body if the record contains information about research being or to be carried out by or on behalf of the private body, the disclosure of which would be likely to expose—</td>
</tr>
<tr>
<td></td>
<td>• the private body; a person that is or will be carrying out the research on behalf of the private body; or</td>
</tr>
<tr>
<td></td>
<td>• the subject matter of the research, to serious disadvantage.</td>
</tr>
<tr>
<td><strong>Section 70</strong></td>
<td>Despite any other provision of this Chapter, the head of a private body must grant a request for access to a record of the body contemplated in section 63(1), 64(1), 65, 66(a) or (b), 67, 68(1) or 69(1) or (2) of the Act if—</td>
</tr>
<tr>
<td></td>
<td>a) The disclosure of the record would reveal evidence of—</td>
</tr>
<tr>
<td></td>
<td>(i) a substantial contravention of, or failure to comply with, the law; or</td>
</tr>
<tr>
<td></td>
<td>(ii) imminent and serious public safety or environmental risk; and</td>
</tr>
<tr>
<td></td>
<td>b) The public interest in the disclosure of the record clearly outweighs the harm contemplated in the provision in question.</td>
</tr>
<tr>
<td><strong>Section 71</strong></td>
<td>The head of a private body considering a request for access to a record that might be a record contemplated in section 63(1), 64(1), 65 or 69(1),</td>
</tr>
<tr>
<td>Legislation</td>
<td>Summary of provision</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>(Notice to Third Parties)</strong></td>
<td>must take all 5 reasonable steps to inform a third party to whom or which the record relates of the request.</td>
</tr>
<tr>
<td><strong>Section 72</strong></td>
<td>A third party that is informed in terms of section 71(1) of a request for access, may, within 21 days after being so informed— make written or oral representations to the head concerned why the request should be refused; or give written consent for the disclosure of the record to the requester concerned.</td>
</tr>
<tr>
<td><strong>Section 72 (Representations and Consent - Third Parties)</strong></td>
<td>A third party that obtains knowledge about a request for access other than in terms of section 71(1) of the Act may make written or oral representations to the head concerned why the request should be refused; or give written consent for the disclosure of the record to the requester concerned.</td>
</tr>
<tr>
<td><strong>Section 80</strong></td>
<td>Despite this Act and any other law, any court hearing an application, or an appeal against a decision on that application, may examine any record of a public or private body to which this Act applies, and no such record may be withheld from the court on any grounds.</td>
</tr>
</tbody>
</table>
| **Electronic Communications and Transactions Act 25 of 2002** | **Definitions**<br>
"access" includes the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data.<br>
"data subject" means any natural person from or in respect of whom personal information has been requested, collected, collated, processed or stored, after the commencment of this Act.<br>
"data controller" means any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject.<br>
"transaction" means a transaction of either a commercial or non-commercial nature, and includes the provision of information and e-government services.<br>
"personal information" means information about an identifiable individual, including, but not limited to-<br>
a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;<br>b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;<br>c) any identifying number, symbol, or other particular assigned to the individual;<br>d) the address, fingerprints or blood type of the individual;<br>ee) the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;<br>f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;<br>g) the views or opinions of another individual about the individual;<br>hh) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the
### Legislation

<table>
<thead>
<tr>
<th>Summary of provision</th>
</tr>
</thead>
<tbody>
<tr>
<td>name of the other individual where it appears with the views or opinions of the other individual; and</td>
</tr>
<tr>
<td>i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but excludes information about an individual who has been dead for more than 20 years;</td>
</tr>
<tr>
<td>“private body” means-</td>
</tr>
<tr>
<td>1. a natural person who carries or has carried on any trade, business or profession, but only in such capacity;</td>
</tr>
<tr>
<td>2. a partnership which carries or has carried on any trade, business or profession; or</td>
</tr>
<tr>
<td>3. any former or existing juristic person, but not a public body.</td>
</tr>
</tbody>
</table>

### Section 50, Protection of Personal Information: Scope of Protection of Personal Information

This Chapter only applies to personal information that has been obtained through electronic transactions. A data controller may voluntarily subscribe to the principles outlined in section 51 by recording such fact in any agreement with a data subject. A data controller must subscribe to all the principles outlined in section 51 and not merely to parts thereof. The rights and obligations of the parties in respect of the breach of the principles outlined in section 51 are governed by the terms of any agreement between them.

### Section 51, Principles for Electronic Collection of Personal Information

**Principles for electronically collecting personal information**

1. A data controller must have the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law.
2. A data controller may not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required.
3. The data controller must disclose in writing to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored.
4. The data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law.
5. The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected.
6. A data controller may not disclose any of the personal information held by it to a third party, unless required or permitted by law or specifically authorised to do so in writing by the data subject.
7. The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed.
8. The data controller must delete or destroy all personal information which has become obsolete.
9. A party controlling personal information may use that personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party.

### Section 86

**Unauthorised Access, Interception,**

86 (1) Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), [RICA] a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.
### Interface with Data

(2) A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence.

(3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence.

(4) A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence.

(5) A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence.

### Electronic Communications and Transactions Act 36 of 2005

#### Section 75

(Data Protection and Privacy)

The Authority may prescribe or impose through licence conditions, as the case may be, measures in respect of directories and directory enquiry services, regarding— the protection of personal data; the protection of privacy.

### National Credit Act, Act 34 of 2005

#### Objects

To promote a fair and non-discriminatory marketplace for access to consumer credit and for that purpose to provide for the general regulation of consumer credit and improved standards of consumer information; ...

#### Part A - Interpretation

‘confidential information’ means personal information that belongs to a person and is not generally available to or known by others.

#### Part B – Confidentiality, personal information and consumer credit records

In the case of an inconsistency between a provision of this Part read with any relevant definition in section 1, and a provision of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000), the provisions of this Part and that Act apply concurrently, to the extent that the provisions of this Part are not excluded in terms of section 5 of that Act.

#### Section 68

(Right – Confidential Treatment)

(1) Any person who, in terms of this Act, receives, compiles, retains or reports any confidential information pertaining to a consumer or prospective consumer must protect the confidentiality of that information, and in particular, must— use that information only for a purpose permitted or required in terms of this Act, other national legislation or applicable provincial legislation; and report or release that information only to the consumer or prospective consumer, or to another person.

### Consumer Protection Act 68 of 2008

#### Definitions

‘consumer’, in respect of any particular goods or services, means—

a) a person to whom those particular goods or services are marketed in the ordinary course of the supplier’s business;

b) a person who has entered into a transaction with a supplier in the ordinary course of the supplier’s business, unless the transaction is exempt
<table>
<thead>
<tr>
<th>Legislation</th>
<th>Summary of provision</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section 11</strong> (Consumer’s Right – Privacy)</td>
<td>The right of every person to privacy includes the right to— refuse to accept; require another person to discontinue; or in the case of an approach other than in person, to pre-emptively block, any approach or communication to that person, if the approach or communication is primarily for the purpose of direct marketing.</td>
</tr>
<tr>
<td><strong>Section 107</strong> (Offences and Penalties)</td>
<td>It is an offence to disclose any personal or confidential information concerning the affairs of any person obtained—in carrying out any function in terms of this Act; or as a result of initiating a complaint or participating in any proceedings in terms of this Act.</td>
</tr>
</tbody>
</table>

**Regulation of Interception of Communications Act 70 of 2002**

<table>
<thead>
<tr>
<th>Objects</th>
<th>To regulate the interception of certain communications, the monitoring of certain signals and radio frequency spectrums and the provision of certain communication-related information.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Definitions</th>
<th>&quot;communication&quot; includes both a direct communication and an indirect communication.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;direct communication&quot; means an—</td>
<td>oral communication, other than an indirect communication, between two or more persons which occurs in the immediate presence of all the persons participating in that communication; or</td>
</tr>
<tr>
<td>utterance by a person who is participating in an indirect communication,</td>
<td>if the utterance is audible to another person who, at the time that the indirect communication occurs, is in the immediate presence of the person participating in the indirect communication;</td>
</tr>
<tr>
<td>&quot;indirect communication&quot; means the transfer of information, including</td>
<td>&quot;indirect communication&quot; means the transfer of information, including a message or any part of a message, whether —in the form of— speech,</td>
</tr>
<tr>
<td>a message or any part of a message, whether —in the form of— speech,</td>
<td>music or other sounds; data; text; visual images, whether animated or not; signals; or radio frequency spectrum; or</td>
</tr>
<tr>
<td>music or other sounds; data; text; visual images, whether animated or</td>
<td>in any other form or in any combination of forms, that is transmitted in whole or in part by means of a postal service or a telecommunication system.</td>
</tr>
<tr>
<td>not; signals; or radio frequency spectrum; or in any other form or in</td>
<td></td>
</tr>
<tr>
<td>any combination of forms, that is transmitted in whole or in part by</td>
<td></td>
</tr>
<tr>
<td>means of a postal service or a telecommunication system.</td>
<td></td>
</tr>
</tbody>
</table>

"intercept" means the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the— monitoring of any such communication by means of a monitoring device; viewing, examination or inspection of the contents of any indirect communication; and diversion of any indirect communication from its intended destination to any other destination.

<table>
<thead>
<tr>
<th>Section 2</th>
<th>Subject to this Act, no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legislation</td>
<td>Summary of provision</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>(Prohibition - Interception of Communication)</td>
<td>To intercept, at any place in the Republic, any communication in the course of its occurrence or transmission.</td>
</tr>
</tbody>
</table>
| **Section 3**  
(Interception of Communication under Interception Direction) | Subject to this Act, any authorised person who executes an interception direction or assists with the execution thereof, may intercept any communication; and postal service provider to whom an interception direction is addressed, may intercept any indirect communication, to which that interception direction relates. |
| **Section 4**  
(Interception of Communication by Party to Communication) | Any person, other than a law enforcement officer, may intercept any communication if he or she is a party to the communication, unless such communication is intercepted by such person for purposes of committing an offence. Any law enforcement officer may intercept any communication if he or she is— a party to the communication; and satisfied that there are reasonable grounds to believe that the interception of a communication of another party to the communication is necessary on a ground referred to in section 16(5)(a), unless such communication is intercepted by such law enforcement officer for purposes of committing an offence. Interception of communication with consent of party to communication. |
| **Section 5**  
(Prior Written Consent) | Any person, other than a law enforcement officer, may intercept any communication if one of the parties to the communication has given prior consent in writing to such interception, unless such communication is intercepted by such person for purposes of committing an offence. (2) Any law enforcement officer may intercept any communication if— one of the parties to the communication has given prior consent in writing to such interception; he or she is satisfied that there are reasonable grounds to believe that the party who has given consent as contemplated in paragraph (a) will— participate in a direct communication or that a direct communication will be directed to him or her; or send or receive an indirect communication; and the interception of such direct or indirect communication is necessary on a ground referred to in section 16(5)(a), unless such communication is intercepted by such law enforcement officer for purposes of committing an offence. |
| **Section 6**  
(Interception of Indirect Communication - Connection With Carrying On Of business) | (1) Any person may, in the course of carrying on of any business, intercept any indirect communication— by means of which a transaction is entered into in the course of that business; which otherwise relates to that business; or which otherwise takes place in the course of the carrying on of that business, in the course of its transmission over a telecommunication system. (2) A person may only intercept an indirect communication in terms of subsection (1) if such interception is effected by, or with the express or implied consent of, the system controller; for purposes of monitoring or keeping a record of indirect communications in order to establish the existence of facts; for purposes of investigating or detecting the unauthorised use of that telecommunication system; or where that is undertaken in order to secure, or as an inherent part of, the effective operation of the system; or monitoring indirect communications made to a confidential voice-telephony counselling or support service which is free of charge, other than the cost, if any, of making a telephone call, and operated in such a way that users thereof may remain anonymous if they so choose; if the telecommunication system concerned is provided for use wholly or partly in connection with that business; and if the system controller has made all reasonable efforts to inform in advance a person, who intends to use the telecommunication system concerned, that indirect communications transmitted by means thereof may be intercepted or if such indirect communication is intercepted with the express or implied consent of the person who uses that... |
See table 2 for other Acts that impact on the processing of personal information.

### Table 2: Other Acts that impact on the processing of personal information

<table>
<thead>
<tr>
<th>Legislation</th>
<th>Summary of provision</th>
</tr>
</thead>
<tbody>
<tr>
<td>The National Archives and Records Service Act No. 43 of 1996</td>
<td>Section 13 requires public bodies to manage their records in a well structured manner through the use of a record keeping system and to implement the necessary policies and procedures to ensure that their record keeping &amp; records management practices comply with the requirements of the Act. Part V of the Regulations to the Act contains the specific parameters within which public bodies should establish and maintain their record management systems.</td>
</tr>
<tr>
<td>The Public Finance Management Act No. 1 of 1999 (PFMA) and the Municipal Finance Management Act No. 56 of 2003 (MFMA)</td>
<td>These Acts regulate the financial management and governance structures of institutions within the national, provincial and local spheres of government. They aim to prevent mismanagement, abuse and corruption by requiring that all government bodies manage their financial and other resources in a responsible and transparent manner. Information is an important resource that must be efficiently and effectively managed similar to money, people and other assets. The idea of information, including personal information, being adequately safeguarded as an important business asset has been reinforced in the recent amendments to the King Code on Corporate Governance (KING III) which is also applicable to the public sector.</td>
</tr>
</tbody>
</table>
The Protection of Personal Information Bill [B2 ... 2009]
4. The Protection of Personal Information Bill [B2 ... 2009] (PoPI)

4.1. Introduction

Privacy in South Africa is currently protected in terms of section 14 of the Constitution, 1996. While there is not yet a particular statute providing for privacy, as required by the Constitution, it is included in several diverse statutes and protected in terms of the common law.

The South African Law Reform Commission (SALRC) approved an investigation into privacy and data protection in 2000. This was followed three years later, by an Issue Paper and subsequently, in 2005 by a Discussion Paper and a draft Bill, published for public comment. In May 2009, the SALRC confirmed that a further draft, together with their Report had been submitted to the Minister of Justice for consideration.

On 13 August 2009 Cabinet approved the Protection of Personal Information Bill (PoPI). PoPI aims to give effect to the constitutional right to privacy by introducing measures to ensure that organisations process personal information in a fair, responsible and secure manner [3]

Once it is passed into law it will attempt to protect individuals by penalising organisations and other parties that fail to take adequate steps to secure personal information such as identity and contact details.

Protection of Information Act

A distinction must be drawn between PoPI and the Protection of Information Act, 84 of 1982 (PIA). The purpose of PIA is to provide for the protection from disclosure of certain information which applies largely to the safety and security of South Africa and its people. In other words, it has to do with information regarded by the Government of South Africa as being of high value and high sensitivity.

PIA is currently before Parliament and deals with the protection of state information. It empowers the government to classify certain information into ‘Top Secret’, ‘Secret’ and ‘Confidential’ categories in order to protect the national interest from suspected espionage and other hostile activities.

State information is any information generated, acquired, received or in the possession or control of the government. This could include various types of information such as personal, sensitive or commercial information. Responsibility for PIA resides with the Department of State Security.
4.2. **Overview of the Protection of Personal Information Bill [B2 ... 2009] (PoPI)**

The preamble to PoPI recognizes the right to privacy as well as the need for economic and social progress in an information society. PoPI seeks to regulate, in harmony with international standards, the processing of personal information by public and private bodies.

Specifically, PoPI seeks to:

- Promote the protection of personal information processed by public and private bodies.
- Introduce information protection principles so as to establish minimum requirements for the processing of personal information.
- Provide for the establishment of an Information Protection Regulator.
- Provide for the issuing of codes of conduct.
- Provide for the rights of persons regarding unsolicited electronic communications and automated decision making.
- Regulate the flow of personal information across the borders of the Republic. [3]

The content and structure of PoPI, is as follows:

- **Chapter 1:** Definition and purpose
- **Chapter 2:** Application provisions
- **Chapter 3:** Conditions for lawful processing of personal information
- **Chapter 4:** Exemption from information protection principles
- **Chapter 5:** Supervision
- **Chapter 6:** Notification and prior investigation
- **Chapter 7:** Codes of conduct
- **Chapter 8:** Rights of data subjects regarding unsolicited electronic communications and automated decision making
- **Chapter 9:** Transborder information flows
- **Chapter 10:** Enforcement
- **Chapter 11:** Offences and penalties
- **Chapter 12:** General provisions
- **Schedule 1:** Laws repealed and amended
4.3. Personally Identifiable Information (PII)

Chapter 1 of PoPI defines personal information (PI) as meaning: “information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment to the person;

(d) the blood type or any other biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person; and

(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person” [3].

Examples of attributes that may include personal information are:

- passport and ID numbers;
- gender and biometric identifiers;
- bank account and credit card numbers;
- birth dates;
- home address details;
- personal telephone numbers for both landlines and mobile devices;
- personal email and IP addresses;
- photographs;
- trade-union membership;
- sexual orientation;
- criminal convictions or committed offences;
- financial profiles;
- personal identification numbers (PINs) and passwords for financial accounts;
- health information;
- race;
- religious or philosophical beliefs;
- age;
- special needs;
- behavioral profiles; and
- information relating to juristic persons, such as the articles of incorporation, shareholder agreements and the like.
There are many variations of personal information for example personal identifiable information (PII), Protected Health Information (PHI), electronic Protected Health information (Ephi), Non-public personal financial information (NPI) and Non-personal identifiable information (non-PII).

Section 25 of PoPI provides for a prohibition on the processing of “special personal information”, which concerns information about a child who is subject to parental control in terms of the law, or a data subject’s religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life or criminal behaviour. Processing of special personal information is subject to a heightened level of protection.

**What is the scope of PoPI?**

PoPI covers the processing of personal information in both electronic and paper-based format. Processing in terms of PoPI means any operation or activity or any set of operations, whether or not by automated means, concerning personal information, including (see figure 1) [3]:

(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as blocking, degradation, erasure or destruction of information.
To whom does PoPI apply?

PoPI applies to any person or organisation (public or private) that processes personal information in South Africa.

PoPI does not apply (see figure 2) [3]:

- to the processing of personal information in the course of a purely personal or household activity;
- when personal information has been de-identified to the extent that it cannot be re-identified again;
- if personal information is processed by or on behalf of the State and (i) which involves national security, defence or public safety; or (ii) the purpose of which is the prevention, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in specific legislation for the protection of such personal information;
- for exclusively journalistic purposes by responsible parties who are subject to, by virtue of office, employment or profession, a code of ethics that provides adequate safeguards for the protection of personal information;
- by Cabinet and its committees, the Executive Council of a province and a Municipal Council of a municipality;
- relating to the judicial functions of a court referred to in section 166 of the Constitution; or
Figure 2: The exclusions of PoPI

Which Government department is responsible for introducing PoPI?
The custodian of PoPI is the Department of Justice and Constitutional Development.

What are the human rights implications of PoPI?
PoPI is meant to give effect to the right to privacy contained in the Constitution. It is meant to protect individual interests against the abuse of power. There is some debate about whether the provisions in the PoPI may conflict with the right of access to information, also contained in the Constitution. However, PoPI contains certain mechanisms designed to maintain a fair balance between these rights.

4.4. The impact of PoPI on the Public Sector

Government departments, constitutional institutions and public entities collect and distribute large amounts of information in the advancement of their public mandates for the public interest. Innovations in information technology and the sheer magnitude of information databases held by the public sector places added strain on the government. Government is tasked to act in a transparent manner by providing access to information; while simultaneously protecting the confidentiality and privacy of citizens and, ensuring alignment with local and international information management standards.

Much of the information contained in public sector databases is personal or sensitive in nature. The cumulative employee database of government is generally amongst the largest of any sector. In addition, much of the information captured, stored and distributed by government is obtained directly from and linkable to specific individuals, businesses and other organisations, such as:

- employment and earnings information for social services and tax purposes;
- citizenship, residence and tourist information;
- criminal records;
• licensing information related to motor vehicle registration and traffic enforcement;
• permit information for building and property purposes;
• information available to agencies dealing with service delivery and utilities billing;
• census information;
• health information; and
• voter information including political affiliations.

The overall accountability for the lawful processing of personal information will have to be formally assigned. To be lawful personal information may generally only be processed for specified, explicit and legitimate purposes in a fair, responsible and secure manner without unreasonably intruding on the privacy of persons. Certain additional safeguards are required for personal information that is deemed sensitive in nature.

Compliance with PoPI is likely to result in significant operational challenges for public sector institutions. However, failure to comply could expose institutions to regulatory fines, criminal prosecution and civil litigation resulting in the award of aggravated damages. There could also be significant loss of trust and reputational damage due to a perceived lack of transparency and accountability in public decision-making.

Certain specific instances of personal information processing within the public sector are excluded from the applicability of PoPI. These exclusions cover the processing of personal information:

• by or on behalf of the State which involves national security, defense or public safety or for law enforcement purposes as long as adequate safeguards have been established in specific legislation for the protection of such personal information;
• by Cabinet and its committees, the Executive Council of a province and the Municipal Council of a municipality; and
• relating to the judicial functions of a court referred to in section 166 of the Constitution [3].
An Overview of the Privacy Principles
5. An overview of the privacy principles

Table 3 provides a summary of the eight principles as well as examples of controls that organisations may consider when addressing these principles.

Table 3: Summary of the eight privacy principles

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
<th>Example controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 1: Accountability</td>
<td>Section 7 of the Protection of Personal Information Bill (PPI Bill) requires a responsible party to ensure that the principles contained in PoPI and the measures that give effect to the principles are complied with. This Principle is titled the Principle of Accountability. In real terms, the Principle of Accountability necessitates assurance that the requirements of PoPI are being implemented. The responsible party (organisation) must be able to evidence controls, safeguards and mechanisms appropriate to the requirements of PoPI. For instance: (i) the organisation should appoint or designate a person who will be responsible for the implementation of PPI policies and procedures (ii) the organisation should develop and implement a Framework and Action Plan that reduces the requirements of PoPI into actionable items and indicates a timeline for implementation of the policies and procedures; (iii) the organisation should show reporting, oversight and sanction in respect of the implementation of the policies and procedures. The Principle of Accountability underpins the purpose of PoPI which is to give effect to the constitutional right to privacy, by ensuring that an organisation adopts internal measures to regulate compliance with PoPI [3].</td>
<td>• Establish the Information Privacy Officer (IPO) or privacy related roles such as for the Legal, Internal Audit, Training and Communications, Risk and Compliance, Marketing, Human Resources, Research and Development, Finance, Information Security, Information Technology and Operations. • Define reporting structures • Define IPO roles and responsibilities • Define a Privacy Framework and action plan • Define a Privacy Policy and Privacy statement. • Update the disciplinary process • Establish monitoring and audit procedures • Consider insurance • Define privacy and security induction training • Define ongoing training such as web based training • Define an awareness program with continuous messages • Assess and improve the Information Protection Culture</td>
</tr>
<tr>
<td>Principle</td>
<td>Description</td>
<td>Example controls</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Principle 2: Processing limitation** | The second principle deals with the lawfulness of processing, minimality of information collected, consent, justification and objection, and the collection of personal information directly from the data subject [3].  
According to this principle, personal information must be processed in a lawful and reasonable manner that does not infringe the privacy of the data subject. It provides further that such processing must be relevant to the purposes for which the personal information was collected by the responsible party.  
Personal information may also only be processed with the consent of the data subject, however consent is not required if the processing is necessary for the conclusion of for example a contract or by law. A data subject may object to the processing of personal information if he or she has reasonable grounds to do so, or if it has been provided for in national legislation. If a data subject does object to the processing of personal information, the responsible party may not further process the information.  
The responsible party must collect personal information directly from the data subject except under certain circumstances provided in PoPI. For example, the responsible party need not collect personal information directly from the data subject if the personal information is in a public record. | • Updated customer applications forms in terms of the information fields, terms and conditions, opt-out and opt-in, responsible party information, etcetera  
• Define lawful processing of PII in organisation  
• Update employee contracts and terms of conditions  
• Update third party contracts  
• Update notices at all points of PII data collection (e.g. website, call centres, etcetera.) |
| **Principle 3: Purpose specification** | The third principle provides that personal information must be collected for a specific purpose and the data subject from whom the personal information is collected must be made aware of the purpose for which the personal information was collected [3].  
This principle also highlights the retention and the destruction/deletion of personal information once the purpose for which the personal information was collected has been achieved. | • Update customer / employee contracts specifying what and why PII is processed as well as by whom  
• Identify what sensitive PII must be collected and why  
• Update the document management policy and retention schedules  
• Identify third parties processing PII of customers /employees  
• Update third party contracts and service level agreements, sign-off addendums  
• Conduct third party due diligence reviews  
• Conduct background checks |
| **Principle 4: Further processing limitation** | The fourth principle regulates the further processing of personal information. If a responsible party further processes personal information, such processing must be compatible with the purpose for which the information was collected in terms of principle 3 [3].  
In order to determine whether further processing is compatible, the responsible party is required to take into account a number of issues. For example, the relationship between the intended purpose by further processing, and the purpose for which the personal information was collected by the responsible party must be considered. | • Define the notification and objection process  
• Define the further possessing request process  
• Define third party reviews and audits |
<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
<th>Example controls</th>
</tr>
</thead>
</table>
| Principle 5: Information quality | The fifth principle provides that the responsible party must take reasonable steps to ensure that the personal information that has been collected is complete, accurate, not misleading and up to date. In so doing, the responsible party must take into consideration the purpose for which the personal information was collected [3]. | • Ensure input validation and integrity checks  
• Implement an update process for data subjects  
• Conduct business process reviews  
• Conduct compliance audits |
| Principle 6: Openness | The sixth principle provides that the responsible party must be open about the collection of personal information by notifying the Regulator if it is going to process personal information and, if personal information is going to be collected, the responsible party must take "reasonably practicable steps to ensure that the data subject has been made aware that his or her personal information is going to be collected. The responsible party should for example, take reasonable steps to make the data subject aware of its name and address, and the purpose for which the personal information being collected [3]. | • Notification of PII processing to Regulator  
• Define a loss and disclosure procedure |
| Principle 7: Security safeguards | The seventh principle provides that the responsible party must ensure that the integrity of the personal information in its control is secured through technical and organisational measures [3]. This principle also extends to anyone who processes information on behalf of the responsible party that is, third parties. Third parties may only process such information with the permission of the responsible party, and must treat such information as confidential. The responsible party must also ensure that third parties processing personal information for it have the technical and organisational measures in place to preserve the integrity of the information. A written contract between the parties should be in place. Security safeguards include the handling of compromises and breaches of personal information belonging to data subjects. For example, responsible parties and third parties that have processed personal information that has been compromised must provide a notice of the breach to the Regulator and the data subject concerned. | • Define a breach notification procedure  
• Implement identity and access management  
• Implement physical access controls  
• Implement disaster recovery and business continuity  
• Implement a destruction process  
• Update systems - include data fields, classification, flagging of opt-out or opt-in  
• Update the incident management process and system  
• Implement a process for updating PI across all systems and third parties  
• Conduct privacy impact assessment for new systems  
• Implement privacy notices on websites, update cookies, implement a P3P  
• Update the Information Security policy  
• Implement cryptography and encryption  
• Implement ISO27001/ISO27002 controls  
• Implement PCI DSS requirements  
• Implement pseudonymous & anonymous controls / procedures  
• Conduct third party due diligence  
• Implement portable device security |
<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
<th>Example controls</th>
</tr>
</thead>
</table>
| Principle 8: Data subject participation | The eighth principle provides that data subjects have the right to request that a responsible party confirm (free of charge) whether it holds personal information about the data subject, and he or she may also request a description of such information [3]. If the personal information is then provided to the data subject, the responsible party must advise the data subject of his or her right to correct or have deleted such personal information in terms of section 23 of PoPI. This principle also looks at any fees the data subject may have to pay to gain access to his or her personal information, as well as the responsible party’s right to refuse to provide the data subject with access to certain records in terms of Parts 2 and 3 of Chapter 4 of the Promotion of Access to Information Act (PAIA, which provide the Grounds for Refusal of Access to Records). The responsible party may also be required to inform all parties to whom the personal information has been disclosed of the steps taken. It is important to note that sections 18 and section 53 of the Promotion of Access to Information Act, (Forms of Request) apply to any requests made under principle 8. | • Data subject access request process  
• Update the PAIA manual |
Establishing an Information Protection Culture
6. Establishing an information protection culture

An organisation’s annual profit may suffer due to information security incidents. A number of data breach studies indicate that insiders pose a threat to the protection of information and could be behind most breaches, whether intentionally or unintentionally.

An organisation can appoint a data privacy officer, launch a privacy program, update its policies and contracts, implement the required technical controls, give employees training in new business processes, but still have data breaches and customer information being lost or accessed by unauthorised people. In many instances the cause of information security incidents can be related to the behaviour of employees, their buy-in, commitment, skills, understanding of requirements and implementation thereof.

Organisations therefore need to pay serious attention to reducing the risk that employee behaviour poses to the protection of information and specifically, personal information.

6.1. What is an information protection culture?

An information protection culture develops as a result of employees’ interaction with information protection controls such as passwords, access cards or anti-virus software and the behaviour they exhibit within the context of the organisational culture in the organisation. Their interaction becomes the way things are done in the organisation to protect information.

The interaction between information security components such as a policy (i.e. requiring shredding or password protection of files) and the behaviour of employees has an impact on the resulting information protection culture. The objective is to instil information protection behaviour that is conducive to the protection of information assets based on the organisation’s information security policies and code of ethics.

The information protection culture can minimise information risks and guide employee behaviour by considering a variety of controls focussing on people, process and technology.

6.2. The impact of PoPI on an information protection culture

South African organisations will have to protect personal information according to the 8 principles specified in PoPI. This means that employees will have to change the manner in which they process personal information from the collection of personal information from the customer (whether through application forms, the internet or call centres) up to the destruction thereof.

In essence, the organisational culture will have to change. The questions that one is faced with are:

- How do organisations change the interaction and behaviour of employees when processing personal information?
- How do organisations ensure that employees follow data privacy policies and implement the new procedures accordingly?
- How do organisations ensure that an information protection culture is cultivated where employees understand and “live” the data protection principles in their daily interaction with personal information?
6.3. Implementing an information protection culture

In order to effectively instil a culture of information protection the organisational behaviour of employees must be considered in the data privacy program that is based on a holistic data protection framework. Some of the key components that must be incorporated in the framework relates to:

- Leadership and governance (e.g. strategy and risk);
- Management and operations (e.g. legal requirements);
- Policies and procedures (e.g. best practice);
- User management (e.g. trust, awareness, training);
- Program management (e.g. monitoring and audit);
- Technology and operations (e.g. technical and physical); and
- Change Management.

The privacy principles and controls must be implemented on 3 tiers in an organisation, namely the organisational tier, group tier, and individual tier. Often organisations concentrate on the organisational tier where strategies and policies are defined as well as on the group tier where group training is implemented. The individual tier is often omitted resulting in unchanged employee attitude and behaviour.

Focussing on employee attitude and behaviour means that one would need to address each privacy principle and integrate it in the above components on all three tiers. Strong emphasis must be placed on buy-in, timely communication, participation from employees in the project, business process reengineering and effective change management programmes. Awareness must be conducted from the initiation of the privacy project and specific guidance provided on how employees need to revise daily operational tasks.

6.4. Measuring an information protection culture

Another effective technique to focus on employee attitude and behaviour is to measure it. This will aid the organisation in the identification of the actual developmental areas per department, job level, region and even age group in the organisation. Action plans and awareness campaigns can then be channelled to address areas where it is most needed and benchmark it year on year for indication of improvement.

To measure employee attitude and behaviour an information protection survey can be conducted. The survey should include questions relating to each component for example:

- There are clear directives on how to protect sensitive customer information.
- I know where to save sensitive customer information.
- I believe management keeps my private information confidential.
- I believe employees are willing to change their work procedures to protect personal information.

It is important to ensure that the questionnaire used in the survey is valid and reliable. This is achieved through statistical analysis (e.g. Structural Equation Modelling and Factor analysis). Statistical analysis is also used to analyse the data and to determine statistical signification differences between biographical groups (e.g. job levels). Software that can be used is for instance Survey Tracker, NCSS and SPSS.

Action plans are identified based on the survey data and a remediation roadmap is compiled to address areas where information protection behaviour must be changed to improve the culture of information protection.

Without information protection components to direct and influence employee behaviour, employees could well interact with information assets in ways that would introduce risk. In time, this potentially harmful behaviour could unfortunately give rise to a culture where neglect is regarded as acceptable. To cultivate an
acceptable level of information protection, organisations should ensure that a comprehensive and adequate set of information protection components is implemented on all tiers in the organisation and specifically on the individual tier. Cultivating a strong information protection culture will ultimately aid organisations to comply with PoPI and to minimise potential incidents.
The Impact of PoPI on Different Industries
7. The impact of PoPI on different industries

PoPI will impact organisations in all industries. Personal information may only be processed within the confines of the strict requirements set out in PoPI.

The result of non compliance to this impending legislation may irreparably harm an organisation’s reputation and customer confidence. Directors are entrusted with ensuring a company executes its compliance requirements. Non compliance is not negotiable for stakeholders.

PoPI will have a huge impact on the manner in which Human Resource Departments process employee information. The recruitment process, employee terms and conditions, appraisal and other related processes will be affected.

The manner in which organisations conduct Marketing will also be affected as organisations will have to obtain the individual’s consent to market products to them.

PoPI affects the manner in which information is transferred across South African borders. This will it affect both multinational organisations and organisations with partners in other countries.

This section provides information specific to the Financial and Insurance sector, Healthcare sector, ICT industry and Public sectors. Some other industries that will also be significantly affected are the Tourism and Leisure industry and the Consumer Market industry.

7.1. Financial and insurance sector

The Financial and Insurance industry is already regulated through legislation such as the National Credit Act, Act 34 of 2005 (NCA) and Financial Intelligence Centre Act, 2001 (FICA) requirements. PoPI will now require that personal information relating to financial data be protected in a similar manner.

Banks and financial institutions are one of the key users of what is termed “personal information”. In order to process personal information, banks, as a responsible party, must comply with the requirements set out in PoPI. The following points pertain specifically to the Financial and Insurance sector:

- Steps must be taken to ensure that the person to whom the personal information relates (the data subject) is aware of the purpose for which the information is collected.
- Security measures must be put in place to protect personal information against loss, damage and unlawful access. If a third party processes information on behalf of a bank, the bank and the 3rd party must conclude a written contract requiring the 3rd party to establish and maintain confidentiality and security measures.
- Records may only be kept for prescribed periods, after which time it must be destroyed or de-identified.
- Steps must be taken to ensure that processed information is complete, accurate, not misleading and kept updated. Therefore, adequate monitoring will be required to ensure that the location of information is known at all times.
- Where reasonable grounds exist that processed personal information has been unlawfully accessed, banks must notify the Regulator and the data subject.
- Individuals will have the right to obtain details regarding their personal information from banks. They may also require the correction of such information.
- Banks must, before sharing information between companies within that banking group, obtain client consent and disclose the purpose for which the information will be shared.
• Any conflict or overlap with other laws or codes having an impact on banks must be identified and managed accordingly.

• Terms and conditions of existing agreements must be reviewed, and client consent obtained where necessary and appropriate.

• The transitional arrangements allow for 12 months following the effective date of PoPI for existing processes to align with the requirements set out in PoPI.

• An information Protection Officer must be registered with the Regulator, and the Deputy Information Protection Officers must be designated and delegated, as necessary.

7.2. Health care sector

There are various pieces of legislation which have direct bearing on the protection of personal health information. They place a responsibility on all role players in the public and private health care environment to ensure the confidentiality of personal health information. Privacy in the private health care environment may include instances where a patient or consumer refuses to permit a health care provider to either disclose or transmit information to any other party not directly involved in the health care delivery process.

This section provides a holistic view of the impact of PoPI in the private health care environment. It examines the information flow between various entities which have a direct and indirect involvement in the provision of health care services.

The information environment

The health care environment is large and complex. The following diagram aims to provide a view of the entities involved and the information that flows between them.

There are four main collection areas in the health care environment. They are the following:

• Providers normally collect personal information during consultation on healthcare for medical records. These are deemed highly sensitive and confidential.

• Medical Schemes collect personal information through application forms and includes demographic, socio-economic, medical and administrative information such as banking details.

• Provider Organisations collect information regarding registered health care practitioners.

• Medical Supply and Distribution Companies collect information relating to medical supply orders and or billing information and in the case where medicines are directly delivered to patients.
Who are the responsible parties?

According to PoPI, a responsible party must exist who ensures that the principles are complied with. From the diagram above we can clearly identify the following responsible parties:

- Medical Schemes;
- Council for Medical Schemes;
- Risk Equalification Fund;
- The Department of Health;
- Health Professions Council of South Africa;
- Group practitioner association & doctor networks;
- Independent Practitioner Association and doctor networks;
- The Hospital Association of South Africa; and
- Private Hospital Groups.
**Health care legislation**

There are additional regulatory requirements we need to consider in the health care environment. Table 4 provides an overview of some of the regulatory requirements.

**Table 4: Overview of health care legislation**

<table>
<thead>
<tr>
<th>Legislation</th>
<th>Who is covered</th>
<th>What is covered</th>
</tr>
</thead>
</table>
| Children Act No.38 of 2005 | Children under the age of 18 | HIV Status  
- No person may disclose the fact that a child is HIV positive without consent from the child > 12 years old, parents or caregivers. |
| Choice on Termination of Pregnancy Act No 92 of 1996 | Female persons under the age of 18 | Abortion  
- Termination of life shall remain confidential at all times, unless the female in question chooses to disclose such information. |
| Electronic Communications and Transactions Act No 25 of 2002 | All natural persons |  
- Express written permission is required for the processing of PII.  
- Disclose in writing is required for the specific purpose for processing.  
- There may be no disclosures to third-parties unless it is permitted by law or specifically authorised to do so in writing by data subject.  
- Unidentifiable or anonymous statistical data can be disclosed to third-parties. |
| Health Act No 63 of 1977 | Medical practitioners |  
- In case of a notifiable medical condition the following data elements must be disclosed to authorities:  
  - Name;  
  - Age;  
  - Sex;  
  - Population Group;  
  - Identity Number;  
  - Date of commencement of notifiable medical condition; and  
  - Place and source of infection. |
| Health Professions Act No 56 of 1974 | Professional Boards |  
- Where patients have consented to treatment, express consent is usually not needed before relevant PI is shared to enable the treatment to be provided.  
- Health Care Providers may disclose PI if the patient is incapable of giving consent because of immaturity or mental capacity.  
- PI may be disclosed in the case of children < 14 with consent from his/her parents /guardians.  
- In the case of a deceased patient with written consent of his/her executor.  
- Psychologists:  
  - May disclose PI only with written informed consent of the patient.  
  - In case when engaging in electronic transmission of PI, that privacy & confidentiality must be maintained. |
| Medical Scheme's Act No 131 of 1998 | Board of Trustees |  
- Accounts or statements **must** contain the relevant diagnostic and such other item code numbers that relate to such relevant health service.  
- A written protocol must be in place that contains provisions for ensuring confidentiality of clinical and propriety information.  
- Any information pertaining to the diagnosis, treatment or health of any medical scheme beneficiary must be treated as confidential. |
<table>
<thead>
<tr>
<th>Act</th>
<th>Natural Persons</th>
<th>Details</th>
</tr>
</thead>
</table>
| Mental Health Care Act No 17 of 2002          | All natural persons | • The person, human dignity and privacy of every mental health care user must be respected.  
• Care may be provided only if:  
  - the user has consented to care;  
  - authorised by Court Order; or  
  - a delay in care will result in death, serious harm or damage.  
• A user cannot receive care unless a written application for care is made to the head of the health establishment.  
• Care can be provided without consent if:  
  - there is reasonable belief that the user is likely to inflict serious harm;  
  - there is a need for the protection of the financial interests or reputation of the user; or  
  - the health care user is incapable of making an informed decision.  
• No psychosurgery may be performed who is not capable of giving informed consent.  
• In the case where a user is incapable of consenting, a curator may consent to the treatment or operation.  
• Consent must be adhered to in the case of electro-convulsive treatment. |
| National Health Act No 61 of 2003             | The person in charge of a health establishment | • Health records must be created & maintained for every user of health services.  
• All information concerning a user is confidential.  
• Disclosure of information may take place, the user consents to that disclosure in writing.  
• Control measures must be put in place to prevent unauthorised access to those records and to the storage facility or system, by which records are kept.  
• The NHA provides for a National Information System, where various categories of data for submission & collection are prescribed by the Minister. |
| Nursing Act No 50 of 1978                     | Nurses           | • The disclosure by a nurse of any information concerning a patient obtained in the course of activities of the nurse, shall constitute an act in respect of which disciplinary steps can be taken. |
| Pharmacy Act No 53 of 1974                   | Pharmacies       | • Disclosure of confidential information obtained in the course of the professional activities of a pharmacist, except with the express consent of the patient, or in the case of a child, the express consent of a parent/guardian, shall be deemed unethical or unprofessional conduct. |
| Promotion of Access to Information Act No 2 of 2002 | All natural persons | • The head of a private body must refuse a request for access to a record of the body if its disclosure would involve the unreasonable disclosure of personal information about a third party, including deceased persons unless the individual has consented in writing where the record is held by a private or public body.  
• Mandatory disclosure in public interest is required if the disclosure of the record would reveal evidence of imminent and serious public safety or environmental risk and the public interest in the disclosure outweighs the harm contemplated. |
| Sterilization Act No 44 of 1998               | Health Care Providers | • Sterilization of a person is allowed if the patient is capable of consenting and at least 18 years old.  
• Sterilization of persons younger than 18 years or persons incapable of consenting requires a parent/guardian/curator’s consent.  
• The person in charge of the facility must be notified of the sterilization and keep record of every such sterilization. |
Impact of PoPI on the health care sector

Consent is required for treatment and not the submission of Protected Health Information (PHI) as required in the National Health Act (Act No. 61 of 2003), (NHA), it is therefore clear that the following information must be given to a patient:

- the reasons or purposes for the disclosure;
- the likely consequences of the disclosure;
- the intended recipients of the PHI; and
- the likely consequences of non-disclosure if the patient is entitled to medical scheme benefits, namely that the medical scheme may elect not to reimburse the claim of the patient.

It seems likely that the NHA and PoPI are in conflict, as non-disclosure of PHI may result in medical schemes not reimbursing health care services.

Information security in the health care environment is a legal obligation. Policies and procedures therefore need to be implemented, and be seen to be implemented, which are designed to ensure the confidentiality of patient data at all stages of processing.

Health care providers should take action to protect the privacy of all patients. The following should be considered:

- accounts and statements should include notices about the uses of PHI;
- contractual agreements which defines confidentiality and non-disclosure practices with third-party providers should be concluded;
- patients should be made aware that PHI will be shared with third-parties, unless the patients decide to opt-out;
- Medical Aid Schemes should review access rights to personal information and security of access to information via the Internet;
- Medical Aid Scheme contracts with members should state the reasons for the disclosure of PHI, and the likely consequences of disclosure and non-disclosure; and
- the names of the Data Management companies who have agreed to data protection requirements in contracts with health care providers should be made visible to data subjects if they require to know with whom PHI will be disclosed.

All medical entities in the health care environment should acknowledge that confidentiality and security of personal information are legal obligations.

7.3. The Information, Communications and Technology (ICT) Industry

The ICT sector has long ago adopted a number of privacy enhancing techniques. The industry has placed value on customer information. Robust risk management strategies have been used to identify and mitigate a number of information risks.

The information age and technology may pose a real threat to the protection of personal information. It is also one of the enablers to safeguard information. The model for protection of personal information will have to address automated and un-automated systems and processes wherein information resides. It will address both the physical and electronic handling path of information and cater for a myriad of information risk management techniques.

Additionally, other risks may be mitigated through data processing agreements, binding corporate rules for adoption and a wide communication campaign to affect behavioural change. The approach therefore may be a
holistic advance to privacy as part of a wider information governance framework. The model will set out roles and responsibilities and a review and reporting structure that will monitor the maturity of the data governance framework.

*Technology to circumvent privacy evolving faster*

There are a number of privacy protection safeguards that seek to prevent unauthorised access and disclosure of personal information. Often external privacy intrusive techniques have developed faster than privacy enhancing tools. The collaborative efforts of large industry players may result in potent defences against information attacks. This in turn may lead to the strategic development of privacy security forums to share and counteract risks to information protection. Consequently, conversations with the global information village may result in further collaborative efforts.

*Privacy strategy*

PoPI will result in the reassessment of privacy strategies in order to satisfy compliance requirements. An enterprise wide solution will serve the requirements set out in the proposed legislation. The impact may be the centralisation of privacy functions across business in order to better serve compliance requirements; segment and establish market differentiation; increase sales; safeguard its reputation and attract and retain its customers. The residence of the Information Protection Officer or Privacy Officer may be Legal or Operational Risk Management. The type of business and nature of its relationship with the Regulator may lead to the strategic development of privacy teams that provide comprehensive management of personal information. The implementation plan will likely be spread over a period of twelve to eighteen months (depending on the Bills effective implementation date). Many private companies have business intelligence analysts who have forecast requirements that have resulted in alignment pre empting the Bill passing into an Act.

*Regulatory partnership and requirements*

A common approach before the passing of any legislation is fervent lobbying with the Regulator. The sector may seek consultation forums with the Information Protection Regulator to facilitate compliance. Healthy dialogue aimed to minimise impact on the bottom-line is important. Subscriber registration (The Regulation of the Interception of Communication and Communication related Information - RICA) was conducted in a similar manner. It is probable that analogous engagements will follow.

Subscriber registration has dented capital expenditure over the past fiscal year with a number of Mobile Virtual Network Operators attributing the drop in profit growth to burdensome compliance requirements in RICA. The intent of the legislation is not to deliberately hinder commercial growth but to give effect to enshrined rights and obligations in principal legislation. We are experiencing an upward legislative spurt that gives effect to third generation rights. The advent of consumerism and the “warned and alarmed” consumer has led to a more knowledgeable consumer stuck in a fight or flight mode.

Thus, the cost of compliance for PoPI will likely be higher in operational resource allocation than on technical development. The sector already enjoys the berths of information security technology and systems to properly manage its information governance framework.

The Operations Privacy team will drive business interest by developing and implementing a privacy system that supports day to day business and provide sound practical solutions. Operational expertise to translate a number of the requirements of the law in this particular industry will result in an insurgence of privacy training. However, operating already in a scarce skills industry may result in limited resources. With diversification of business models in traditional ICT sector trade, an increasing number of products and services entering the market are not conventional voice offerings. Some of the diversified products introduced recently are borne from strategic alliances or partnerships with financial institutions, social networking sites, etcetera.
Hence the build up to implementation of PoPI will result in a flurry of activity to identify and source credible skills to support the Information Protection team. Businesses may strive to capitalise on existing resources in order to contain costs.

**Value proposition**

Major industry role players have long ago established that with stagnant customer growth figures and a saturated market, the draw card is to diversify its products and services. The criteria for choosing a Mobile Virtual Network Operator (MVNO) has predominately been price and coverage. The primary objective of PoPI is notification; consent and choice and information security. Trust will be critical to the relationship between the service provider and the data subject/customer. The customer will be able to exercise more control over the collection and uses of personal information.

Customers invest their information and may reap rewards from this investment. The primary use of the information (the purpose for which it was collected) may be extended to better serve the customer through targeted products and services. The PoPI defines the parameters for primary and secondary uses and respect for the expression of choice and consent of the data subject. Privacy policies and permitted businesses uses will be defined to ensure that the information serves growth potential as well as meet compliance requirements. Businesses are fast realising monetary the value of personal information.

### 7.4. The South African public sector

Increasingly, governments and other public as well as private organisations collect vast amounts of personal information about individuals for a variety of purposes. With the development of new information and communication technologies, the ability of the state and the private sector to collect, record and "mine" personal information has grown exponentially.

**Empowerment of individuals**

Access to information and services empowers individuals and creates value for money. The public service is committed to continuous, honest and transparent communication with individuals. This involves communication of services, products, information and problems, which may hamper or delay the efficient delivery of services to promised standards.

Many improvements that the public would like to see often require no additional resources and can sometimes even reduce costs. Failure to give a member of the public protection of their personal information may result in compromise of information which results in the exposure to liabilities.

Individuals must be allowed to access, challenge and correct information about themselves collected by departments in the course of their statutory activities. This applies both to information collected in paper copy or electronic form (i.e. online). Individuals must be informed about who is collecting the information, why the information is being gathered, and for what purposes it will be used. The collection of personal information must be:

- collected by government institutions in support of their statutory mandates or departmental activities;
- collected from the individual personally;
- accurate and up to date;
- subject to inspection and correction by the individual;
- used only for the purpose for which it was originally collected;
- gathered with the knowledge and consent of the consumer;
- collected for a reasonable purpose; and
- handled and stored securely.
The requirements for implementing PoPI are:

- strategic review of the nature and extent of a privacy structure within the Department;
- strategic planning of the establishment of a privacy structure (including objectives, targets, performance indicators and timeframes and action plans);
- development and implementation of a privacy structure within Departments (policy formulation, procedures, processes, functions responsible for driving and implementing the establishment of a privacy structure and culture within Departments);
- designation of a structure to handle privacy issues and complaints. For the most part, disputes regarding the collection, storage and use of personal information should be resolved this way, between the individual and the department;
- transforming service delivery by incorporating privacy initiatives;
- develop and implement appropriate measures to protect the private details of individuals, captured in either hard copy or electronic form;
- monitoring, evaluation and performance measurement of compliance to PoPI and internal regulations including the production and use of accurate management information statistics;
- communication, consultation and participation with all relevant role players and stakeholders. Given the vital importance of representativeness it is important to ensure that the unions, relevant stakeholder groups and other interested parties are actively involved in the monitoring process. Individuals should be afforded the opportunity to participate in the decision making process on issues affecting the protection of their information;
- developing an effective communications strategy and structures to ensure that the Department’s stance on privacy, accompanying regulations and performance measures;
- establish a financial resource strategy to support the establishment of a privacy structure to ensure adequate financial resources taking into account the specific responsibility of the department and the needs of individuals;
- establishing an effective research strategy and structures to support research into appropriate privacy models;
- building its own capacity in terms of human resources and training to ensure the implementation of a privacy structure, both nationally and provincially;
- establishing effective mechanisms for the co-ordination of privacy policies and programs;
- promoting inter-departmental collaboration in terms of the protection of personal information (i.e. SARS or Home Affairs);
- the installation of new information systems to ensure measures to ensure protection of personal information. This will require investment in equipment and in the training of users, as well as running and maintenance costs;
- putting measures in place to ensure compliance to internal privacy regulations and the PoPI through any outsourcing arrangement, contracts and licenses (i.e. privacy clauses into a contract or license).
- development and implementation of a set of principles governing the storage, collection, security, use, handling, archiving, disclosure, observation and correction of personal information;
- creating an individual complaints mechanism;
- creating departmental sanctions for serious, flagrant or repeated violations of information privacy principles or privacy codes; and
- awareness raising and training strategies designed to promote a positive view of compliance to PoPI.
Government Departments need to constantly measure the extent to which citizens are satisfied with the service or products they receive. It also plays a critical role in the development of service delivery improvement plans to ensure a better life for all South Africans. If privacy is going to survive in the technological age, individuals, groups and institutions must be able to determine for themselves, when, how and to what extent information about them is communicated to others.
PoPI and Trans Border Personal Information Flows
8. PoPI and Trans Border Personal Information Flows

While national laws and policies differ, there is common interest in protecting privacy and individual liberties, in a manner not inconsistent with the free flow of information and the movement of people, goods and services that allow free trade. Nations must comply with domestic legislation while at the same time cooperating internationally.

Some examples of global trans-border requirements are:

- Organisation of Economic Cooperation and Development – Member countries should only restrict trans-border flows of personal information if the other country does not substantially observe the OECD Guidelines.
- Council of Europe – A party to the Convention may not prohibit or require special authorisation for the transfer of information to another Convention country, solely in order to protect privacy.
- 1995 European Union Data Protection Directive – Trans-border transfer of personal information is only permitted if the receiving country ensures adequate levels of protection.
- United States Safe Harbour – Operates only between the United States and the European Economic Area. Notice (informed decision-making) and choice (ability to control), apply. Sensitive information requires explicit opt-in.
- Asia-Pacific Economic Cooperation – Consent of the individual should be obtained where personal information is transferred to third parties, domestically or internationally. Due diligence and reasonable steps are required to ensure that the recipient will protect the information consistent with the APEC Principles.

The Memorandum on the Objects of the Protection of Personal Information Bill, 2009, which emanates from the South African Law Reform Commission’s report on privacy and data protection, records that the purpose of the legislation is to give effect to the right to privacy, by introducing measures to ensure that the personal information of individuals (data subjects) are safeguarded when processed by responsible parties and to balance the right to privacy against other important rights such as the right of access to information, while allowing for the free flow of information within and across the borders of the Republic.

Chapter 9, section 69 of the draft currently publically available, provides for trans border information flows of personal information outside the Republic as follows:

“\textbf{A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless -}"

\textbf{(a) the recipient of the information is subject to a law, binding code of conduct or contract which -}

\begin{enumerate}
  \item effectively upholds principles for reasonable processing of the information that are substantially similar to the information protection principles; and
  \item includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;
\end{enumerate}

\textbf{(b) the data subject consents to the transfer;}

\textbf{(c) the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject’s request;}

\textbf{(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or}

\textbf{(e) the transfer is for the benefit of the data subject, and -}
(i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; and

(ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.”[3]

Chapter 6, section 50 provides for notification to the Regulator prior to processing, in instances of fully or partly automated and non-automated processing of personal information, requiring, the notification to be listed in a register kept by the Regulator and recording, among others, the planned trans border flows of personal information.

It is clear from the above that the proposed South Africa privacy legislation is in line with international standards for cooperation and trans border flows of personal information, requiring the recipient to be subject to a law, binding code of conduct or contract that upholds privacy principles that are substantially similar to the South African principles even relating to further transfer, or, where the individual consents, transfer is necessary and/or in the interests of, or for the benefit of the individual.
The Business Units That Will Be Affected Most
9. The business units that will be affected most

9.1. Legal and Regulatory

Legal and Regulatory departments should ensure that all information management requirements stipulated in applicable legislation and regulations have been identified and communicated to applicable business units.

9.2. Governance, Risk and Compliance

Governance, Risk and Compliance divisions could own the information privacy management programme. They are responsible for monitoring and ensuring operational compliance with applicable legislation, regulations and standards. They must ensure that:

- privacy statements and policies are in place in the organisation;
- responsibilities towards the protection of personal information are assigned and communicated, to internal and applicable external parties (e.g. service providers);
- information lifecycle policies, standards and procedures are defined and implemented, and specifically include criteria for technical security requirements as well as defining the lifespan of personal information in the organisation (i.e. retention periods);
- business practices are compliant with any applicable privacy legislation and regulations;
- business practices related to personal information are compliant with the organisation's privacy statements and policies;
- access to information is managed in accordance with the privacy statement and policy;
- any deviations between statements, policies and practice are identified and rectified;
- processes and procedures are defined to respond to privacy-related requests by data subjects; and
- processes and procedures are defined to respond to and report on security breaches of personal information.

Governance, Risk and Compliance can take overall responsibility and accountability for privacy management in the organisation.

As owners of the Privacy Management Programme, Governance, Risk and Compliance must ensure that business units understand privacy requirements, that business processes are reviewed and amended in line with privacy requirements, and that any funding requirements for system, application or process re-engineering are catered for.

9.3. Information Technology

Information Technology departments must ensure the availability of appropriate supporting technology to facilitate secure access, processing, storage and disposal of personal information:

- technical policies, standards and procedures support data and information privacy objectives;
- appropriate preventative controls (e.g. identity and access management) are embedded into technical systems to ensure security of data and information;
- appropriate detective controls (e.g. security event and incident monitoring) are implemented to detect unauthorised access to or usage of personal information; and
• systems are in place to monitor and report on access and usage of personal information, for audit purposes as well as reporting to or by the Data and Information Privacy Officer.

During initial implementation of the organisation's privacy management programme, IT may be required to update existing policies, standards, procedures and systems, to ensure alignment with privacy management objectives.

9.4. Human Resources Development and Training

All staff should be adequately trained and understand their responsibilities towards personal information. Specific emphasis should be given to staff requiring access to sensitive personal information, such as call centre staff and HR support staff.

Recruitment and placement practices should be reviewed to ensure that staff with access to personal information is appropriately screened before being given access to sensitive information or systems. Staff should also explicitly confirm their understanding of information privacy requirements, before placement as well as periodically during employment.

Employment and non-disclosure agreements should specifically refer to the protection of certain categories of classified information, and should be applicable to all users. The scope of these agreements should extend beyond termination of employment, to give legal recourse in the event of information disclosure after retirement, resignation, redeployment or retrenchment.

9.5. Procurement Services / Vendor- and Third-Party Management

Vendor and third-party agreements should specifically include privacy requirements of personal information which may be accessed, processed or stored by the third-party on behalf of the organisation. Agreements should address information security and privacy requirements on the third-party, and should apply to all applicable vendor systems and users accessing this information. The requirement to protect personal information should extend to information throughout its life cycle.

9.6. Marketing

Marketing departments should only use personal information which was specifically gathered for marketing purposes, or to which the data subjects have given consent for the use for marketing purposes. Marketing departments may use aggregated, de-identified information which contains personal information but which cannot be associated with an individual data subject, for purposes of market analysis and insight, as well as for development of product and service offerings.

Marketing departments should ensure that any information sources used to gather personal information inform data subjects about the intended uses of the information. Data subjects must make informed decisions when providing personal information.

Sales and marketing staff should exercise caution when referring to existing or potential clients, customers or subscribers, e.g. during product presentations. References should only be made with the consent of the affected clients, and references should only provide aggregated statistics or information that has been de-identified.
9.7. Product and Service Development

Product and Service development departments should integrate privacy management into the product and service development process, as well as into the specific products and services being developed. Products and services gathering personal information should:

- disclose the nature of the information being collected to the data subject;
- inform the data subject of the intended use(s) of the information being gathered;
- provide mechanisms for data subjects to give or revoke consent for the gathering of the information; and
- advise the user on processes to query, update or remove their personal information.
The People, Process and Technology Considerations When Implementing Privacy Requirements
10. The people, process and technology considerations when implementing privacy requirements

The requirements of PoPI have an impact on the technical controls, processes as well as human interaction with personal information in the organisation. The following section provides an outline of some of the people, process and technology components that organisations can consider to include as part of their privacy programme.

It should be noted that the people, process and technology components do not represent an exhaustive list, and that each organisation will have to decide which components are required for their specific business to allow for compliance with PoPI. Listed below in Table 5 are examples of privacy guidance documents and frameworks that organisations can use when defining their privacy framework and people, process and technology components.

Table 5: Privacy frameworks and standards

<table>
<thead>
<tr>
<th>Framework / Standard</th>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>GAPP – Generally Accepted Privacy Principles Framework 2006</td>
<td>Provides guidance to design and implement privacy practices in an organisation.</td>
<td>Business and Practitioners version: <a href="http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/default.aspx">http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/default.aspx</a></td>
</tr>
</tbody>
</table>
| ISO/IEC 29100 - Information technology — Security techniques — Privacy framework | “This International Standard provides guidance concerning information and communication technology requirements for the processing of personally identifiable information by:
(a) establishing common privacy terminology;
(b) categorizing privacy preferences and requirements;
(c) referencing known privacy principles; and
(d) relating all described information privacy aspects to existing security guidelines.” | [http://www.iso.org](http://www.iso.org) |
| ISO/IEC 29101 - Information technology -- Security techniques – Privacy reference architecture | “This International Standard provides a high-level reference architecture for planning and building information and communication technology (ICT) systems that facilitate the proper handling of personally identifiable information (PII).” | Under development with a target publication date of 2013-05-15 |
10.1. People components

The effectiveness of the privacy program is dependent on employees who will be required to understand the privacy requirements and implement it. Employees across departments and in various job levels will be affected. There must be a focus on employees (people) in the privacy strategy and program to ensure that employees buy-in, are committed and value the organisations strategy, vision and implementation plan for privacy. The various people components that must be considered are outlines in Figure 4.

Figure 4: People components

1. Exco and management commitment

The executive committee and senior management should understand their responsibility and accountability towards the privacy programme. They need to understand that even in terms of King III they can be held accountable for the protection of personal information as information is an important business asset and risks affecting it must be controlled.

2. Ownership and accountability

Assigning ownership of and accountability for data privacy and protection through a data governance program.

Creating an information strategy that enables the organisation to identify, track and control how data flows across all areas of an organisation’s systems and processes.
3. Business value

Making Data Privacy and Protection a Core Business Value that is integrated in the business strategy.

The development of organisational culture, which includes a data protection culture, develops when top management or managers defines a vision or philosophy and business strategy to implement. People in the organisation will behave in certain ways and be guided by the philosophy and strategy. They will behave according to what is perceived as correct and acceptable and specific organisational behaviour will surface.

It is therefore crucial that the data protection culture becomes a core business value of the organisation and that management’s vision and business strategy includes the protection of information. Management commitment and support is vital to instil a data protection culture to direct employee behaviour.

A culture of acceptance (to change) can only be cultivated from the top down. This can be achieved by management showing active involvement and subscription to said policies. They will lead by example to ensure that users do not have an easy way out of these new situations.

4. Policy acceptance

The data protection policies in the organisation are the cornerstone for creating compliance. The policy must be compiled with all stakeholder input including applicable external parties and unions. All users must sign-off acceptance to the policy to ensure accountability for their actions.

5. Training and awareness

Various learning methods such as e-learning, training and education should be deployed to further cultivate an information protection culture. User education, tracing of user interaction with a Learning Management System as well as the successful completion of a testing module can be considered.

Outcomes-based education can also be considered as a means to address knowledge and attitude in a holistic manner so as to positively influence the information protection culture in an organisation.

Special awareness activities can also be implemented on global privacy and information security awareness days - examples listed in table 6.

Table 6: Privacy and information security awareness days

<table>
<thead>
<tr>
<th>Awareness Day</th>
<th>Date</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Privacy Awareness Week</td>
<td>First week in May</td>
<td><a href="http://www.privacyawarenessweek.org">http://www.privacyawarenessweek.org</a></td>
</tr>
</tbody>
</table>
6. Culture, attitude and behaviour

A data protection culture is “the shared values (‘what is important’) and beliefs (about ‘how things work’) that people in the organisation have about information protection as well as the assumption about what behaviour is acceptable and what not (‘the way we do things around here’). The behaviour exhibited can result either in the protection of information or in incidents compromising the protection of information.

The level of data protection culture develops as a result of top management direction that influences employee behaviour which is the output of the culture. Organisations need to implement the defined people components in order to influence employee behaviour and attitude to instil an acceptable level of information protection culture.

7. Change management

People resist change and therefore change management must be considered when information protection and privacy procedures are implemented.

8. Monitoring

The information security and privacy procedures and measures implemented by organisations should be evaluated on a continuous basis to ensure constant improvement. The following are examples of monitoring activities that can be deployed:

- a data protection culture assessment;
- web based training tests;
- time taken to resolve incidents;
- the number of helpdesk enquiries relating to privacy;
- the number of incidents and losses; and
- sweeping offices to ensure clean desk policies, secure cable locking of laptops, etcetera.

10.2. Process components

One of the areas of focus which an organisation will have adressed once they defined their compliance requirements, as stated in PoPI, focuses on the process dimension of the organisation. This section highlights some of the intricate detail which should be considered when an organisation is addressing privacy requirements, emphasising that real effort will be required.

General best practise driving governance in an organisation focuses on enabling an ongoing process through which an organisation can identify and plan, define and implement, verify and act (See figure 5).
In general, most of what needs to be executed in an organisation follows a process or is underpinned by a process of some nature. These processes provide a vehicle to drive execution based on a defined set of actions, which allows organisations the means to drive adherence. This understanding has been utilised to describe some of the key processes below which are to be considered by organisations when implementing privacy requirements.

**Identify and plan**

Identify the required risks which need to be addressed and plan how to address them.

**Table 7: Process components – Governance and plan**

<table>
<thead>
<tr>
<th>Governance phase</th>
<th>Process components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification of personal</td>
<td>Identify what PI and where PI is processed within the organisation, based on what</td>
</tr>
<tr>
<td>information</td>
<td>is defined as PI by the legislation.</td>
</tr>
<tr>
<td></td>
<td>Possible business departments which might store PI would be:</td>
</tr>
<tr>
<td></td>
<td>• IT;</td>
</tr>
<tr>
<td></td>
<td>• Finance;</td>
</tr>
<tr>
<td></td>
<td>• Human Resources;</td>
</tr>
<tr>
<td></td>
<td>• Call Centres;</td>
</tr>
<tr>
<td></td>
<td>• Marketing Departments;</td>
</tr>
<tr>
<td></td>
<td>• Sales Departments; and</td>
</tr>
<tr>
<td></td>
<td>• Third Parties.</td>
</tr>
<tr>
<td></td>
<td>During the identification process it would be prudent to generate a register of the</td>
</tr>
<tr>
<td></td>
<td>various pieces of PI identified, how they are processed and the information</td>
</tr>
</tbody>
</table>
Governance phase | Process components
---|---
Classification associated with each.

Inventory of categories of personal information | A possible category schema which can be used in the PI identification process:
- **Identity**: PI that can uniquely identify a data subject;
- **Identity Attribute**: a subset of an identity which cannot be used to uniquely identify a data subject;
- **Attribute Set**: Makes up all the elements of an identity;
- **Inferred attribute**: is not itself collected, but generated by processing PI;
- **Preference**: Associated with an identity;
- **Profile**: collection of attributes that can discover and be used in the matching of identities by other entities;
- **Skills Profile**: Associated ratings of a particular set of competencies of a profile;
- **Personal Statement**: Unstructured set of text associated with an identity or profile; and
- **Assertion Records**: Are assumptions or statements made about an identity or profile.

PI risk assessment | **PI Risk assessment** is also known as a Privacy Impact Assessment. A Privacy Impact Assessment (PIA) is a process which enables organisations to anticipate and address the likely privacy impacts of new initiatives, foresee problems, and negotiate solutions to ensure data protection compliance [11].

Risks can be managed through the gathering and sharing of information with stakeholders, allowing them to understand the impact of the risk and what mitigating actions can be introduced to counteract. Systems can be designed to avoid unnecessary privacy intrusion, and features can be built in from the outset, that reduces privacy intrusion.

Where the success of a project depends on people accepting, adopting and using a new system, process or program, privacy concerns can be a significant risk factor that threatens the return on the organisation's investment. In order to address this risk, it is advisable to use the PIA as a risk management technique [11].

**Define and implement**
Define the required controls needed to mitigate the identified risks and implement them via processes into the organisation. Table 8 lists some governance concepts in support of the Define and Implement concept.

**Table 8: Process components – Define and Implement**

<table>
<thead>
<tr>
<th>Governance phase</th>
<th>Process components</th>
</tr>
</thead>
</table>
| Governance construct | In establishing governance the following aspects should be considered to help support the derived processes:
- **Responsibility & Accountability**: Organisation clearly states responsibility for protecting personal information entrusted to them.
- **Objectives**: Governance defined for organisation provides the reference for employees by which they are to conduct business operations while ensuring compliance to controls which safeguard personal information.
- **Monitoring and Management**: The application of the governance is measured in the ongoing application of the controls and the management thereof in the organisation. |
<table>
<thead>
<tr>
<th>Governance phase</th>
<th>Process components</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Legal Implications: The governance framework establishes the platform which drives compliance to various legal constructs. This platform will serve as the interpretation of the organisation of the various pieces of legislation impact on the organisation.</td>
<td></td>
</tr>
</tbody>
</table>
| Policy | In defining the relevant controls required to address the identified risk, it is suggested that the organisation define a policy which encapsulates it interpretation of the required controls. A suggested policy framework could comprise out of the following aspects:  
  * **Purpose**  
  * **Background**  
  * **Scope**  
  * **Roles & responsibilities**  
  * **Policy objectives**  
    * Collection of Private Information  
    * Use and Disclosure of Private Information  
    * Quality of Personal Information  
    * Security of Personal Information  
    * Personal Information Retention  
    * Openness regarding Personal Information  
    * Access to and Correction of Personal  
    * Trans-border flows of Personal Information  
  * **Deviations from policy**  
  * **Monitoring**  
  * **Reporting**  
  * **Disciplinary code of practice and litigation** |
| Data handling procedures | All PI data should be supported by a Data Handling procedure, which allows for the safe handling and storage of information throughout its lifecycle.  
This procedure should allow for the correct identification of the information, thus requiring that an Information Classification be associated with the information. This classification will be used throughout the organisation to allow for correct identification and subsequent treatment of the information items.  
Each Information Classification category should have clearly defined treatments or controls to be applied during the creation, use, storage and destruction of the information, in line with the risk mitigation to be applied to PI.  
These procedures are to be well documented and communicated to ensure adherence to them throughout the organisation. |
| Notifications to regulator | A notification is to be provided by the organisation, before processing of personal information to the Regulator. This is done as part of the requirement around openness of processing and ensuring that the organisation has addressed the stated requirements for collection and processing of information, prior to processing:  
The notification must contain the following particulars [3]:  
1. The name and address of the responsible party;  
2. The purpose of the processing;  
3. A description of the categories of data subjects and of the information or categories of information relating thereto;  
4. The recipients or categories of recipients to whom the personal information may be supplied;  
5. Planned trans border flows of personal information; and  
6. A general description allowing a preliminary assessment of the suitability of the information security measures to be implemented by the responsible party to |
<table>
<thead>
<tr>
<th>Governance phase</th>
<th>Process components</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ensure the confidentiality, integrity and availability of the information which is to be processed.</td>
</tr>
<tr>
<td></td>
<td>It is to be noted that a responsible party will only have to give notice once, and not each time personal information is received or processed.</td>
</tr>
<tr>
<td></td>
<td>Changes in the name or address of the responsible party must be notified within one week and changes to the notification which concern subsection processing of information must be notified in each case within one year of the previous notification, if they are of more than incidental importance.</td>
</tr>
<tr>
<td></td>
<td>Any processing which departs from that which has been notified in must be recorded and kept for at least three years.</td>
</tr>
<tr>
<td></td>
<td>It is important to note that various industries could have additional rules being applied in this regard.</td>
</tr>
<tr>
<td>Privacy notice</td>
<td>The Personal Information Management System (PIMS) shall incorporate procedures to trigger the notification procedure and to ensure that such notifications are kept accurate and up-to-date.</td>
</tr>
<tr>
<td></td>
<td>The PIMS shall incorporate procedures for maintaining records of privacy notices and online privacy statements. These records shall be retained for at least as long as the personal information to which they relate is retained.</td>
</tr>
<tr>
<td></td>
<td>The PIMS shall incorporate procedures which ensure that, where the organisation collects personal information directly from an individual, any privacy notice or online privacy statement required to be given to the individual is provided or made available to the individual prior to any personal information being collected.</td>
</tr>
<tr>
<td></td>
<td>The PIMS shall incorporate procedures which ensure that the content of any privacy notice or online privacy statement is presented in a way which allows it to be easily understood by, and accessible to, its intended audience.</td>
</tr>
<tr>
<td></td>
<td>NOTE Privacy notices intended to be used with the collection of personal information from vulnerable adults, people with learning difficulties or children need to be presented in a language and format which are readily understandable and are accessible to them. [1]</td>
</tr>
<tr>
<td>Retention process</td>
<td>The PIMS shall reference retention schedules for personal information which shall:</td>
</tr>
<tr>
<td></td>
<td>1. Include any minimum retention periods required by law, as well as by the organisation;</td>
</tr>
<tr>
<td></td>
<td>2. Make clear the justification and basis for the retention periods; and</td>
</tr>
<tr>
<td></td>
<td>3. Document any applicable justification for retaining personal information for a longer period than the stated minimum retention period, e.g. where it might be retained for historical and/or research purposes.</td>
</tr>
<tr>
<td></td>
<td>The PIMS shall incorporate procedures for the implementation of the retention schedules and the communication of the schedules to all relevant workers.</td>
</tr>
<tr>
<td></td>
<td>The PIMS shall incorporate procedures which ensure that personal information no longer required by the organisation is disposed of.</td>
</tr>
<tr>
<td></td>
<td>The PIMS shall incorporate or reference disposal procedures which are managed:</td>
</tr>
<tr>
<td></td>
<td>• using approved processes;</td>
</tr>
<tr>
<td></td>
<td>• with a level of security appropriate to the sensitivity of the personal information; and</td>
</tr>
<tr>
<td></td>
<td>• in line with the organisation’s information security risk assessment. [1]</td>
</tr>
</tbody>
</table>
| Third party contract process | Parties engaging with a Third Party should firstly define the extent to which the engagement would impact on personal collected information. Where personal information is involved the company who wishes to engage in the contract must ensure that the explicate consent received during the collection process of the personal information provides for the contracting of a third party. Further to this,
where this third party operates outside of the borders of South Africa, it is to be
ensured that the explicate consent obtained allows for the personal data to be
transported cross-border.

The contract engagement process should be initiated with the signing of Non-
Disclosures, to protect the sharing of information during the contractual
engagement.

As part of the formal contracting process with a Third party, the company is to
perform a due diligence on the security principles employed by the Third Party. The
objective is to ensure alignment and conformance to the same measures in
protecting the personal information. In addition to this the company establishes a
base to manage risk in relation to the personal information, which can lead to
additional contractual obligations which are to be stipulated and honoured by the
Third Party. This becomes crucial in trans boarder information flows, as the
legislative context in the Third Parties country might not align, nor provide adequate
stipulation to ensure the risk is managed. Thus the contract between the two entities
needs to ensure that this risk is addressed.

Contract should stipulate:

1. Responsible parties in both contracting parties who carry the accountability for
security of personal information in line with contractual agreement.

2. Define the measures to be used to verify that controls support contractual
agreement. Measures are to be associated with forms of evidence which can be
used to manage disputes. These measures should be tied to a Service Level
Agreement to support contractual engagement.

3. Review cycles of agreement and controls.

4. The process to follow to address breaches in respect to personal information.
   This is to include notice and remediating action.

Contract should ensure supporting liability cover to address potential breaches in
security or contract. Here to extent of cost to be incurred to repair incident (such as
customer communication) is to be considered.

On a practical note the information flow process is to be documented and
understood to the extent that changes in personal information consent can be
communicated between the organisation and the Third Party, keeping in sync with
the persons personal preferences, as it pertains to the personal information
collected.

**Procedure for ensuring quality of PI (internal and third parties)**

In order to ensure on a continuous basis a sufficient quality of the PI data, the
accountable entity should have in place internal systems and procedures covering the
following three areas [10]:

1. **Data quality management**
   - **1.1.** Data quality management is a continuous process that should include the
     following steps:
     
     1.1.1. **Definition of the data** (identification of the business needs in terms
           of data, a detailed description of the data items, including attributes,
           entities, etcetera, that should be collected and the relations
           between the different data items);

     1.1.2. **Assessment of the quality of data**, i.e. the verification of the data
           quality criteria for the purposes of analysis and decision making. The
           assessment of data quality should have due regard to the quality and
           performance of the mechanisms (i.e. channels) used to process
           (refer to the definition in the draft bill) data, in particular when data
           is provided by third parties;

     1.1.3. **Remediation activities based on business impact and materiality**, i.e.
           the material problems identified during the verification process
           should be solved within appropriate time frames and with the view
           to improve the current data processes to ensure the quality of future
           data; and

     1.1.4. **Monitoring data quality**. This involves the monitoring of the relevant
           systems used to process data. The monitoring process could be
<table>
<thead>
<tr>
<th>Governance phase</th>
<th>Process components</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>based on key performance indicators, but expert judgement must play a key role in the analysis.</td>
</tr>
<tr>
<td>2. Internal activities on the processing of PI.</td>
<td></td>
</tr>
<tr>
<td>2.1. The following principles are relevant:</td>
<td></td>
</tr>
<tr>
<td>2.1.1. Data should be classified and maintained on a comprehensive basis;</td>
<td></td>
</tr>
<tr>
<td>2.1.2. The level of granularity of data must be in line with the purpose; and</td>
<td></td>
</tr>
<tr>
<td>2.1.3. Historical data should be kept based on purpose.</td>
<td></td>
</tr>
<tr>
<td>3. The role of internal/external assurance providers</td>
<td></td>
</tr>
<tr>
<td>3.1. The role of both the external auditors and internal assurance providers requires that some degree of analysis is performed with regard to the quality of the data.</td>
<td></td>
</tr>
<tr>
<td>Incident management</td>
<td>A process is to be defined to address incidents which occur pertaining to the personal information. This process should provide the following steps:</td>
</tr>
<tr>
<td>1. Identify the criteria which would classify an incident.</td>
<td></td>
</tr>
<tr>
<td>2. Define the various categories of incidents, and their associated criticality.</td>
<td></td>
</tr>
<tr>
<td>3. Define the impact of the incident and the remediating action.</td>
<td></td>
</tr>
<tr>
<td>4. Implement the remediating action and verify that risk has been averted.</td>
<td></td>
</tr>
<tr>
<td>5. Conclude incident resolution with a close out report.</td>
<td></td>
</tr>
<tr>
<td>6. In case where severity of incident requires notification of regulator, instigate relevant process to notify regulator.</td>
<td></td>
</tr>
<tr>
<td>Data access request</td>
<td>1. A formal access request form is to be established which is to be completed for each data request, clearly stating the person request the data and for which purposes this request is made.</td>
</tr>
<tr>
<td>2. This request is submitted to the person responsible for the data, or other identified accountable individual for approval. Approval is provided based on the organisations governance requirements in line with the legislative requirement, as it pertains to the requested data.</td>
<td></td>
</tr>
<tr>
<td>3. If the request is approved, verification of the approval is provided, based on purposes described in request.</td>
<td></td>
</tr>
<tr>
<td>4. The requestor must ensure that the data is adequately protected in line with classification of data.</td>
<td></td>
</tr>
<tr>
<td>Data collection process</td>
<td>The data collection process should include the following components:</td>
</tr>
<tr>
<td>1. Clearly articulate purposes for which information is collected.</td>
<td></td>
</tr>
<tr>
<td>2. Person from whom information is collected must authorise the collection and use of information.</td>
<td></td>
</tr>
<tr>
<td>3. Authorisation of collection of information is to be retained and linked to the record retention process.</td>
<td></td>
</tr>
<tr>
<td>4. Collected information is labelled as to ensure that it is recognisable for handling and protection purposes.</td>
<td></td>
</tr>
<tr>
<td>5. Applicable logical and physical access controls are applied to collected information.</td>
<td></td>
</tr>
<tr>
<td>Process to address employee contracts</td>
<td>A process is to be defined and established to address the employees in the organisations contracts, ensuring that they are contracted with the relevant obligation to protecting personal information. A suggested process could comprise out of the following steps:</td>
</tr>
<tr>
<td>1. Define if current employee contracts adequately convey protection and responsibility for the handling of personal information.</td>
<td></td>
</tr>
<tr>
<td>2. If not, built into employee contract relevant disclosure to align with legal requirement, as it pertains to employee</td>
<td></td>
</tr>
<tr>
<td>3. Provide relevant awareness and training to educate employees on additional responsibility and effort required from them. In addition the consequences of non-adherence is to be highlighted to the employee</td>
<td></td>
</tr>
</tbody>
</table>
Verify

Verify that the implemented controls are driving behaviour of organisational resources to conform to the required compliance levels.

Table 9: Process components - Verify

<table>
<thead>
<tr>
<th>Governance phase</th>
<th>Process components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>Compliance is established by addressing the following three main aspects:</td>
</tr>
<tr>
<td></td>
<td>1. Establish a function to monitor the conformance in the organisation in line with required levels of compliance. This function should maintain a level of objectivity to ensure accurate and impartial reporting.</td>
</tr>
<tr>
<td></td>
<td>2. Define the monitoring frequency for assessment to verify compliance in the organisation. Should at least assess on an annual base, but where there is higher risk associated the organisation might want to increase the frequency.</td>
</tr>
<tr>
<td></td>
<td>3. All compliance assessment should establish a body of evidence to help substantiate the findings from the assessment.</td>
</tr>
</tbody>
</table>

Act

Act on deviations from the required behaviour or outcomes, to be readjusted to drive to stated compliance levels.

Table 10: Process components – Act

<table>
<thead>
<tr>
<th>Governance phase</th>
<th>Process components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk remediation plan</td>
<td>Once it has been identified that a control is not performing as desired to mitigate risk, as remediating action plan should be devised. The objective of the plan is to drive action to mitigate the residual risk identified in a controlled manner.</td>
</tr>
</tbody>
</table>

The above discussion highlights various aspects and processes which are to be considered by organisations in addressing privacy requirements. It is to be noted that adherence does not only lie in the conformance to specific requirements, but also the execution thereof in a systematic manner.

10.3. Technology components

Principle seven of PoPI requires responsible parties to ensure the integrity of personal information under its control and to ensure the reasonable technical and organisation measures are implemented “to prevent any loss of, damage to or unauthorised destruction of personal information; and unlawful access to or processing of personal information”.

Use of standards and frameworks

There are various information security standards and frameworks available that organisations can use to implement information security controls to protect the integrity, confidentiality and availability of personal
information. It is important to also follow a risk based approach when implementing technical controls. ISO 27001 and ISO 27002 define an overarching security framework consisting of 133 specific controls that organisations can implement through the application of a risk management process. It is important for organisations to identify the threats to personal information which could be intentional (e.g. hackers) or unintentional (e.g. errors). There could also be vulnerabilities that exist from a process (e.g. ineffective access management) or technology (e.g. unsecured network) perspective. The threats and vulnerabilities result in information security risks that affect personal information.

The above mentioned standards can be used by organisations to apply a step by step process to select the appropriate security controls to mitigate the risks in their environment. Other standards such as Control Objectives for Information and Related Technology (Cobit), and the Standard of Good Practice (SOGP) from the Information Security Forum (ISF) can also be used and integrated to provide a holistic approach to implement information security.

**Technology controls**

Many of the controls (components) adopted and implemented by individuals and/or companies are driven through technology. The technical controls can consist of preventative, corrective or detective controls. The technical controls can be implemented on various levels in an organisation for example the network, hosts and operating systems, middleware, applications and clients and devices. Organisations should have an understanding of their technical environment to identify the components where risk resides in order to implement the correct technical controls.

Choosing the best fit solution based on the risks and regulatory requirements is one of the most important steps. There are a number of questions organisations can ask to assist when dealing with privacy from a technology perspective:

- Who is accountable for protecting the organisation’s personal information?
- Are there any policies defining what measures are to be taken to protect personal information?
- How does your organisation manage incidents relating to privacy breaches?
- How does your organisation protect personal information at rest and in transit?
- How does your organisation protect personal information residing outside your organisation?
- Who has access, how do they access and from where do they access the personal information?
- How does your organisation monitor and track access and changes to personal information?
- How does your organisation ensure the secure availability of the personal information i.e. business continuity and disaster recovery plans?
- What personal information is available on non-production platforms i.e. backup facilities, development and test platforms?
- What controls are in use to effectively dispose of personal information?

Figure 6 lists some considerations that can aid organisations when implementing technical controls.

Figure 6: Technology component considerations

1. ASSESS - Define the project scope to reduce cost
2. SECURE - Focus on Quick Wins
3. COMPLY - Combine overlapping projects to reduce cost
4. RESPOND - Be Prepared. Minimise damage by responding faster

a. Where is my personal information located?
b. What devices contain personal information?
c. Who has access to my personal information?
d. These fundamental aspects of information security can help an organisation rapidly improve its security stance generally without major procedural, architectural, or technical changes to its environment.
e. Watch out for insiders, particularly system administrators.
f. By thinking smart, organisations can integrate their compliance efforts into a single project that reduces the overall cost of compliance.
g. What is the action plan in the event of a security incident?
h. How do I reduce the time to detect and respond to a security incident?
i. The use of audit logging may pay dividends in avoiding compromise and shortened response time in the future.

Twenty critical technology controls

There are different techniques to apply technology controls. From an architecture point of view one can consider aspects such as to limit unique identifiers and common attributes across databases or to store contact information separate from transaction information. One could also automate audits of the collection of personal information for instance to monitor cookie usage and to monitor data flows to and from the organisational website. Table 11 contains 20 critical controls that support technical controls.

The SANS Institute has released the [7] Top 20 critical security controls for cyber defence, that were agreed to by a consortium of agencies including: US National Security Agency, US Cert, US Department of Defence Joint Task Force-Global Network Operations, the US Department of Energy Nuclear Laboratories, US Department of State, US Department of Defence Cyber Crime Center plus the top commercial forensics experts and pen testers that serve the banking and critical infrastructure communities. The consensus effort that has produced this document has identified 20 specific technical security controls that are viewed as effective in blocking currently known high-priority attacks.
### Table 11: Technical Controls

<table>
<thead>
<tr>
<th>Top critical controls</th>
<th>Supporting technical controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory of Authorised and Unauthorised Devices</td>
<td>Asset management and tracking</td>
</tr>
<tr>
<td>Inventory of Authorised and Unauthorised Software</td>
<td>White listing, Least privilege</td>
</tr>
<tr>
<td>Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers</td>
<td>Encryption, Patches. (Secure Build)</td>
</tr>
<tr>
<td>Secure Configurations for Network Devices such as Firewalls, Routers, and Switches</td>
<td>Do not use vendor supplied passwords for system passwords &amp; other security parameters (Non-default configuration)</td>
</tr>
<tr>
<td>Boundary Defence</td>
<td>Install &amp; Maintain a Firewall to protect PI</td>
</tr>
<tr>
<td>Maintenance, Monitoring, and Analysis of Security Audit Logs</td>
<td>Track &amp; Monitor all access to network &amp; PI data</td>
</tr>
<tr>
<td>Application Software Security</td>
<td>Develop &amp; maintain secure systems &amp; applications (SDLC, OWASP)</td>
</tr>
<tr>
<td>Controlled Use of Administrative Privileges</td>
<td>Role based administration, Independent audit of super users</td>
</tr>
<tr>
<td>Controlled Access Based on Need to Know</td>
<td>Restrict, control and monitor access to stored PI data at the source</td>
</tr>
<tr>
<td>Continuous Vulnerability Assessment and Remediation</td>
<td>Regularly test security systems &amp; processes</td>
</tr>
<tr>
<td>Account Monitoring and Control</td>
<td>Assign a unique ID to each person with computer access, Identity and access management</td>
</tr>
<tr>
<td>Malware Defences</td>
<td>Use &amp; update anti-malware software</td>
</tr>
<tr>
<td>Limitation &amp; Control of Network Ports, Protocols, and Services</td>
<td>NAC/NAP, Syslog, Netflow</td>
</tr>
<tr>
<td>Wireless Device Control</td>
<td>802.1x, WPA ,IDS/IPS, Roque detection</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>Discovery, Classification, Report and prevent, Rights Management, Encryption</td>
</tr>
<tr>
<td>Incident Response Capability</td>
<td>Incidence response plan</td>
</tr>
<tr>
<td>Data Recovery Capability</td>
<td>Back up strategy</td>
</tr>
<tr>
<td>Technical physical access controls</td>
<td>Access Control (RFID), CCTV, Device Encryption, Geographic location, HVAC</td>
</tr>
<tr>
<td>Penetration testing</td>
<td>Regular physical &amp; network security reviews</td>
</tr>
<tr>
<td>User Awareness training</td>
<td>Training of staff in privacy procedures and to resist social engineering attacks</td>
</tr>
</tbody>
</table>

### Privacy Enhancing Technology (PET)

Privacy Enhancing Technologies (PET) refers to a range of technologies that can be applied to protected personal information. Table 12 provides an overview of some PET controls that can be considered.

### Table 12: Privacy Enhancing Technology (PET)

<table>
<thead>
<tr>
<th>PET controls</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymisation of personal data</td>
<td>Depersonalising personal information through software that does not record personal information or destroys it after collection and verification.</td>
</tr>
<tr>
<td>Biometrics</td>
<td>Methods used to uniquely recognise individuals based on one or more intrinsic physical or behaviourial trait (e.g. retina scan fingerprint). Biometrics can be used to identify authorised used who require access to personal information.</td>
</tr>
<tr>
<td>Data discovery and classification</td>
<td>Automated technology exists that will search through your data storage systems looking</td>
</tr>
<tr>
<td>PET controls</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PET controls</td>
<td>for personal information, that may exist within your environment. This technology requires you to describe the personal information, such as a 13 digit Identity Number, and then point it at your data storage. Data storage that can be searched includes databases, email systems, file servers and web based portals, such as Microsoft SharePoint.</td>
</tr>
<tr>
<td>Data masking</td>
<td>Data masking is the process whereby sensitive data is preplaced with fictitious data.</td>
</tr>
<tr>
<td>Data encryption</td>
<td>Encryption can be placed at various levels for instance on the applications or database level, the file system or disks (e.g. external media).</td>
</tr>
<tr>
<td>Database Activity Monitoring (DAM)</td>
<td>DAM is an important technology for protecting sensitive databases from external attacks by cybercriminals. According to Gartner, “DAM provides privileged user and application access monitoring that is independent of native database logging and audit functions. It can function as a compensating control for privileged user separation-of-duties issues by monitoring administrator activity.” [6]</td>
</tr>
<tr>
<td>Data reduction</td>
<td>Reduction is the process whereby sensitive personal information in a document is blacked out, based on your role within the organisation and your level of “need to know”. E.g. financial administrators don’t need to know personal medical information.</td>
</tr>
<tr>
<td>Incident response automation</td>
<td>Incident response is something that should be prepared for before an incident occurs. There are numerous tools available that can assist with evaluating your incident readiness. If you can respond to an incident more quickly, you can reduce the damage that an attacker is able to inflict.</td>
</tr>
<tr>
<td>Logical access</td>
<td>Logical access is the use of computer controls for identification, authentication, authorisation, and accountability when users require access to information or systems. User access to personal information must be controlled as well as the rights they have in terms of processing personal information under their profile.</td>
</tr>
<tr>
<td>Online Privacy Notices</td>
<td>Online privacy notices are required on websites where personal information is processed. The privacy notice should for instance state the information that is collected via the website, the uses of the information and the choices customers have. The privacy notices must be easy to find and at or before the point of collecting personal information. It is important to address the use of cookies in the privacy statement. Choices should be provided for the use of cookies and no plaintext personal information should be included in cookies.</td>
</tr>
<tr>
<td>Permissions management</td>
<td>Complex file system permissions may result in unauthorised exposure of sensitive information. In order to better manage this risk it is crucial to deploy automated tools that audit data access activity, fix and maintain access controls, identify sensitive data, find data owners, and involve them in access review and authorisation processes.</td>
</tr>
<tr>
<td>Platform for Privacy Preferences Project (P3P)</td>
<td>P3P is a machine readable policy format containing the privacy statement of the website in XML that web browsers can read. Other examples of machine-readable languages are Application Preference Exchange Language (APPEL) and Enterprise Privacy Authorisation Language (EPAL).</td>
</tr>
<tr>
<td>Quality Enhancing Technologies (QET)</td>
<td>Technology used to ensure the completeness and accuracy of data as well as whether the data is up to date.</td>
</tr>
<tr>
<td>Separation of data</td>
<td>Separation of data refers to the manner in which personal information is saved. For example personal identifying information (identity information) is saved in one domain and all other personal data (health or financial information) in another. Software is used to control the access to the various domains and the authorisation to link data.</td>
</tr>
<tr>
<td>Test Data Management</td>
<td>Application Testing environments typically have less stringent controls to protect them. This means that personal information stored in these environments are exposed to a higher level of risk. Test data management technologies are designed to address these risks by obfuscating personal information, whilst simultaneously enabling application testing for quality and reliability by maintaining its relational context to create error and boundary conditions.</td>
</tr>
</tbody>
</table>
How personal information is lost

The 2010 Verizon Data Breach Investigations Report [8], based on a first-of-its kind collaboration with the U.S. Secret Service, has found that breaches of electronic records last year involved more insider threats, greater use of social engineering and the continued strong involvement of organised criminal groups. With the addition of Verizon’s 2009 caseload and data contributed by the Secret Service - which investigates financial crimes - the report covers 900-plus breaches involving more than 900 million compromised records.

Figure 7 summarises the findings of this report, and shows the number of incidents in the caseload (i.e. how data was compromised) and the size of the dot represents the impact of the data compromise (i.e. the total number of records lost).

Figure 7: Verizon report – Breaches [8]
The Price of Non-Conformance
11. The price of non-conformance

Over the past few years, a number of incidents occurred where people fell prey to the theft and misuse of their identities, proof of which can be found when doing an internet search on the topic of “Identity Theft”.

Although negligence or user naivety could be attributed to many of the incidents, the risk of organised crime to conduct fraud should not be under estimated.

A significant portion of corporate assets are now in the form of information. Assets, such as proprietary processes and customer information, are rising in importance as we shift to an economy more dependent on information. At the same time, more private information—such as health care information and customer identification credentials—is being stored and transmitted online. Both confidential company information and private personal information must be protected.

Table 13 provides an overview of the drivers for privacy as well as examples of the impact of the non-compliance of each driver.

**Table 13: Privacy drivers**

<table>
<thead>
<tr>
<th>Growing scope (drivers)</th>
<th>Impact of non-compliance</th>
</tr>
</thead>
</table>
| Increase in awareness of privacy rights leading to a demand for their privacy. | • Victims suing for damage (legal action).  
• Penalties. |
| Published privacy-related incidents have raised the awareness on the responsibility of Information Owners to protect personal information. | Publicly disclosed security breaches, especially the loss of personally identifying information, can damage brands in the following ways:  
• Demand for the product or service is diminished. In many cases, consumers can easily substitute other products and services for one from a company perceived to be responsible with customers’ personal information.  
• The competitive value of a brand is harmed when a security breach occurs. Even if competitors are just as insecure, the public disclosure of a breach at one company may lead some to assume their competitors are more secure.  
• It is important to note that in the past security breaches could be kept confidential as companies were not required to disclose such incidents. PoPI will however require companies to report all breaches, further increasing the risk of damage to the brand leading to irreparable harm. This may lead to a drop in shareholder confidence. |
| New laws (and cross border business) will force organisations to expand the privacy function. | • Inability to take on international business due to non compliance.  
• Violations in Privacy Legislation may result in triggering other regulations such as the Gramm-Leach-Bliley Act (GLBA) of the US, which also addresses privacy, amongst other issues, in the banking industry specifically. |
| It is becoming easier to access information in an unauthorised manner due to weak authentication mechanisms. | The financial consequences of information leaks manifest themselves directly and indirectly.  
• **Direct losses** occur when revenue is lost as the result of an information leak.  
• **Indirect losses** occur when a competitive advantage is compromised due to an information leak. As noted earlier, those conducting industrial espionage can target IT vulnerabilities to steal information. |
11.1. Statutory offences

Chapter 11 of PoPI [3] sets out the statutory offences attached to the requirements and the associated penalties, namely:

- Hindering, obstructing, or unlawfully influencing the Regulator or the Regulator’s designate may be subject to a fine or imprisonment for a period not exceeding 10 years or to both a fine and imprisonment.
- Other offences such as failing to comply with an enforcement notice issued by the Regulator may be subject to a fine or imprisonment for a period not exceeding 12 months or both a fine and imprisonment.

Interestingly, a Magistrates Court is awarded jurisdiction to issue the penalties imposed by PoPI.

Civil Action

Section 94 [3] provides that a data subject or Regulator acting on behalf of a data subject may institute civil action for damages in respect of a breach of any provision of the PPI Bill.

The court may award an amount as damages for compensation for patrimonial (monetary losses) and non-patrimonial loss (non monetary loss expressed as monetary loss such as pain and suffering) suffered by an aggrieved data subject; aggravated damages (for humiliation, embarrassment etcetera.); interest; and the costs of the lawsuit.

11.2. The privacy scorecard

In considering a risk scorecard for privacy, a number of risks and the associated impact (cost of non-compliance) can be determined [4, 5]:

- Compromise by third parties having access to company information being non-compliant and therefore a weak chain in the link.
- Increase in negative audit findings.
  - Impact: Reputational Damage.
- Increase in high impact and high likelihood risks.
- Degraded customer trust index.
- Loss of competitive advantage
- Delay in taking on new business initiatives.
  - Impact: Financial and Reputational Damage.
- Delay in the execution of key projects or programmes.
  - Impact: Financial
A general perception (label) of non-compliance to standards that should have been complied without the specific direction provided by the Privacy Bill for example, the International Standardisation Organisation Standard ISO/IEC 27002.

- Impact: Reputational Damage.

11.3. Some data breach incidents in South Africa

Table 14 provides an overview of some of the data breaches that occurred in South Africa.

Table 14: Data breaches/incident in South Africa

<table>
<thead>
<tr>
<th>Description</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>On 8th March 2011, the Hawks arrested 6 people on allegations of fraud related to e-filing claims. The fraud scheme was committed by Metropolitan employees who had “easy access” to customers’ personal information.</td>
<td>Estimated loss suffered by SARS could be R1 billion. Known losses were approximately R70 million in a single month attributed to the fraud scheme.</td>
</tr>
<tr>
<td>MWEB Business announced that 1,000 MWeb Business customers’ accounts were briefly compromised on 25 October 2010.</td>
<td>It was claimed that the integrity of the personal information related to the accounts remained intact, and only the username and password of accounts was breached. The actual cost of the forensic investigation has not been released, nor has the estimated cost incurred to contact all the affected customers.</td>
</tr>
<tr>
<td>Zurich Insurance lost an unencrypted data backup tape in transit containing 46,000 UK customers’ personal information and over 500,000 South African customers’ personal information. (October 2008)</td>
<td>In August 2010, the UK Financial Services Authority issued a reduced fine of £2 million. This equates to a fine of approximately R478 per Personal Information record.</td>
</tr>
</tbody>
</table>

Whilst there have been numerous breaches of databases containing credit card details in South Africa, none of these have been officially confirmed. The PCI DSS requirements to protect this information take effect from 30 June 2011, however there has not been any indication as to when merchants will face fines for failure to protect this information in South Africa as of yet. Refer to the ISG Cyber Crime Special Interest Group for updated information. (www.isgafrica.org)
The Benefits of Privacy Compliance
12. The benefits of privacy compliance

12.1. Know your customers

Principle 5 of PoPI mandates organisations to ensure information quality, regarding their customers’ personal information. This includes ensuring that the information is complete, accurate and up to date. This can best be achieved by implementing a Data Governance Program.

Data Governance is a quality control discipline for adding new rigor and discipline to the process of managing, using, improving and protecting personal information. Effective data governance can enhance the quality, availability and integrity of a company’s data by fostering cross-organisational collaboration and structured policy-making.

The effectiveness of highly targeted marketing campaigns is dependent on the accuracy and completeness of customer information. Therefore there is a substantial return on investment that can be achieved from the increase in data quality provided by effective Data Governance including:

- produce more accurate and comprehensive information from and across the enterprise consistently over time;
- protect corporate information to keep auditors and regulators satisfied;
- improve data quality to retain customers and drive new business opportunities;
- control silos of self-interest to benefit the common good of the overall company; and
- directly impact the three factors any organisation most cares about:
  - increased revenue;
  - lowered costs; and
  - reduced risk.

12.2. Know where your customers' personal information is located

Procter & Gamble, often cited as a leader in data privacy, is committed to understanding where its personal information is located. The company has identified and monitors data repositories within the organisation that contain personal data of individuals in 14 categories. – “12 Questions Every GC Should Ask, Corporate Executive Board, 2007” [9].

The key benefits to this strategy include:

1. The ability to build a single version of the truth regarding your customers’ profile.
2. Enhance the protection of personal information because you know where it is, and are therefore able to take a risk based approach to deploy effective controls.
3. Improved ability to monitor who has access to your clients’ sensitive personal information.
4. Mitigate the risk posed by third parties and better manage your service level agreements.
5. Prevent the theft of critical personal information by your competitors, staff, or contractors.
6. Mapping your data flows and creating a data inventory.
12.3. Keep your customers

It is a well known fact that the cost involved in obtaining a new customer is substantially higher than the cost involved in retaining an existing customer. Cyber-espionage is already an everyday occurrence in South Africa, and there is a substantial benefit to a competitor who is able to cherry-pick your most lucrative clients, from inside your very own customer database.

In order to prevent this it is vital to ensure an effective Data Governance Program, based on continuous improvement; proper data protection principles; and the deployment of adequate security systems to protect critical databases.
Conclusion
13. Conclusion

South Africa has emerged in the recent years as a global leader in the African renaissance. We are renowned as an African economic powerhouse; a sustaining economy that has not borrowed money from the International Monetary Fund in the past few years and a persuasive force to be reckoned with in the African Union. The economic and social transformations has ultimately resulted in the South African Legislature passing some of the most progressive legislative reforms for implementation in a democratised, competitive economic sphere. “The world is but our oyster” is the most descriptive and poignant manner to assess the opportunities our young democracy is faced with and with these opportunities so too arise risks and rewards.

The impact of growth and development has resulted in a number of new threats that must be addressed. The Protection of Personal Information Bill has listed a number of privacy commitments that must be attended to. The principles in PoPI are the ethos that drive key privacy deliberations and are central to the implementation of an effective information governance structure. The statements echo the following internationally progressive principle:

- Transparency: Clear communications and practices for privacy that must demonstrate openness and trust.
- Respect: People value their privacy and in turn their privacy ought to be valued.
- Choice: Unequivocal determination of whether or not information may be shared lies with the data subject (person to whom the information relates).
- Accountability: Every user of personal information must be held accountable and responsible for his/her actions in the information governance framework.
- Balance: The information must be used lawfully and in the interest of the data subject and the user (commercial prospectus). Additionally, the information must be used to serve legal duty and the duty imposed as a custodian of information.
- Privacy by design: Privacy considerations should be considered at the outset of the design of any initiative; product or service. It may not be treated as an afterthought or enhancing feature once the activity has been completed
- Legal requirements and industry standards: The compliance requirements to laws; regulations and standards for the protection of personal information are not negotiable. Concurrently, regulatory engagement is vital to achieving this end.

The commentary presented represents expert opinions on the risks that the proposed legislation generates. Academics may postulate that the law is a reaction to growing privacy threats whilst others may agree that the new risks are as a result of growing compliance requirements. These requirements are becoming increasingly more difficult to satisfy. Regardless, some of the privacy risks that have been tabled at the International Working Forum for privacy [2] include the following:

- advertising and analysis of data;
- web privacy and mobile applications (wasps etcetera);
- law enforcement assistance and Regulatory compliance;
- geo location based services;
- surveillance and interests of national security;
- communications monitoring and interception;
- children’s privacy;
- cloud computing; and
- social networks.
Privacy Enhancing Techniques (PET’s) are used as a vital component to meet privacy obligations. The deliberation of which technique to adopt will often be determined by costing models and commercial value propositions. The cost of compliance does not necessitate the use of expensive technology but the use of ordinary common sense. These techniques will be tailored innovative responses to privacy management strategies.

Internationally, our markets differ in terms of legal; political and cultural norms. The widespread commonality is that privacy is a fundamental human right. In some markets the legal structure is provincial and each state mandates laws that support federal requirements. In other markets, a singular legal structure is used to create the basis for this fundamental right. The political and cultural maturity of a country determines the models used. The South African model is highly dependent on cultural influences to privacy.

Therefore, privacy management is more than managing compliance requirements. It must encompass the wider assessment and management of privacy threats and incident handling. An effective model for privacy must include a strategic and operational plan of action. The privacy management system must continuously identify, assess, prioritise and mitigate privacy risks on both a strategic and operational level. On a strategic level, it is key to consider external factors such as legal; regulatory; consumer; political and competition risks. The mitigation strategy and solution will assist in delivering on an organisations commercial strategy. This however is not a once over exercise. Regular evaluation is required to determine the effectiveness of the control activity. All of these must be recorded and reported to ensure that it gets the desired consideration. Included in this model are both internal and external assurance providers and industry expert opinion. This exercise should also cater for organisational consciousness; education and cultural reorganisation in order to appropriately support a robust information governance scheme. This connotes that policies, procedures, practices and organisational structures designed to provide assurance that a risk is managed and that undesired incidents are prevented (a preventative control), or detected (a detective control) and corrected (a corrective action).

The impact of PoPI is multi-stratums. Both the private and public locales of business will be affected. The health care industry collects and stores an immense amount of personal data that must be handled appropriately. The financial sector uses information to determine the eligibility of an individual for important grants such as housing and motor vehicle financing. The national and international crime fighting operations use this data to investigate and apprehend criminals. The marketing industry uses data for commercial appeal through profiling activities. The numerous examples are not exhaustive. It’s used as a foundation to espouse the variants for the legitimate uses for personal information. The legal obligation is to ensure these uses are within what is deemed as legally permissible. Some concerns on privacy are on the outer periphery of privacy compliance requirements or in areas that are yet to be addressed by the South African legislature. It’s incomprehensible that the passing of PoPI will address the multitude of privacy risks we face today. The law creates a legislative framework for compliance.

The cost of non compliance with the proposed Bill is significant. The damage will be commercial (financial losses that may be quantified) and other losses that may not be immediately quantifiable (lack of consumer confidence; reputational and brand harm; consumer churn; civil claims etcetera). It is a reasonable supposition that compliance is not negotiable and organisations must be equipped properly to deal with this pertinent legislation.
Glossary
## 14. Glossary

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymisation</td>
<td>A process by which information directly or indirectly identifying an individual is altered or removed from a collection of PII [1].</td>
</tr>
<tr>
<td>Data Subject</td>
<td>The person to whom personal information relates [3].</td>
</tr>
</tbody>
</table>
| Personal Information                     | “means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—
   (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
   (b) information relating to the education or the medical, financial, criminal or employment history of the person;
   (c) any identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment to the person;
   (d) the blood type or any other biometric information of the person;
   (e) the personal opinions, views or preferences of the person;
   (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
   (g) the views or opinions of another individual about the person; and
   (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.” [3]. |
| Personal Information Management System (PIMS) | “Part of the overall management framework that establishes, implements, operates, monitors, reviews, maintains and improves the management of personal information.” [1]. |
| Protection of Personal Information Bill (PoPI) | To promote the protection of personal information processed by public and private bodies; to introduce information protection principles so as to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Protection Regulator; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters connected therewith [3]. |
| Processing                                | “Means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—
   (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
   (b) dissemination by means of transmission, distribution or making available in any other form; or
   (c) merging, linking, as well as blocking, degradation, erasure or destruction of Information” [3]. |
| Regulator                                 | The Information Protection Regulator established in terms of the requirements in PoPI [3].                                                   |
| Responsible Party                         | 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 [3]. |
| Sensitive Personal Information            | “personal information relating to the individual’s:
   a) racial or ethnic origin;
   b) political opinions;
   c) religious or other beliefs; |
<table>
<thead>
<tr>
<th>Terminology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>d) membership of a trade union;</td>
<td></td>
</tr>
<tr>
<td>e) physical or mental health or condition;</td>
<td></td>
</tr>
<tr>
<td>f) sexual life; and</td>
<td></td>
</tr>
<tr>
<td>g) commission or alleged commission of any offence, including any proceedings, the disposal of such proceedings or the sentence of any court in such proceedings for any offence committed or alleged to have been committed by the individual.”</td>
<td>[1]</td>
</tr>
</tbody>
</table>
References
15. References


[3.] The Protection of Personal Information Bill [B9-2009]
The Protection of Personal Information Bill, 9 of 2009 of South Africa is available for download together with the corresponding briefing papers from the website of the Parliamentary Monitoring Group of South Africa: http://www.pmg.org.za/bill/20090825-protection-personal-information-bill-b9-2009

[4.] Data Privacy, What, When and Where, Paul Strauss (CSSP, CISM), May 2009 (Presentation)

[5.] The Definitive Guide to Information Theft Prevention, Dan Sullivan, Realtime Publishers (Publication)


[7.] “20 Critical Security Controls” is available at https://www.sans.org/critical-security-controls/


