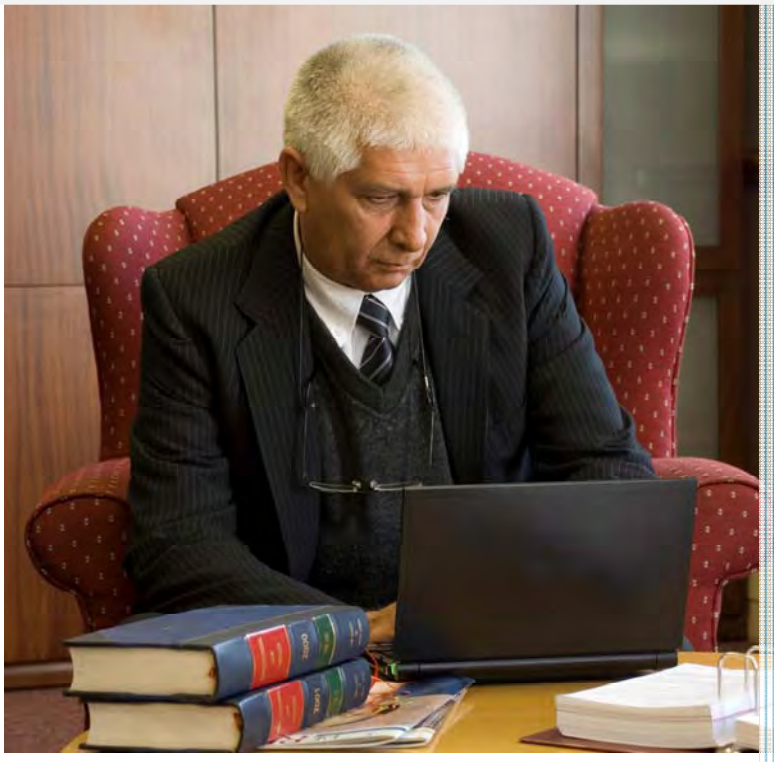
LAW SOCIETY
OF SOUTH AFRICA

Protection of Personal Information Guidelines for Law Firms



Drafted for the
Law Society of South Africa
by Mark Heyink

Protection of Personal Information for South African Law Firms

LSSA Guidelines

VERSION 1.0

MARK HEYINK

Attorney, Notary & Conveyancer
Specialising in Information Law

Foreword

Please read this Foreword carefully.

This guideline has been compiled for the Law Society of South Africa primarily as a tool to assist attorneys in familiarising themselves with their obligations to lawfully process personal information in terms of the Protection of Personal Information Bill.

This guideline is not intended and must not be construed as establishing any legal obligation. Neither is the guideline intended, nor must it be construed, as providing legal advice. Each practice is different and will have to apply the principles which have been developed to protect personal information as may be appropriate and in accordance with the nature of the information and the purpose for which the personal information may be processed.

The Protection of Personal Information Bill as recommended to the Minister of Justice by the South African Law Reform Commission is currently before the Parliamentary Portfolio Committee of Justice and Constitutional Development. The Bill has been shaped and amendments made in response to representations made to the Parliamentary Portfolio Committee and to achieve the Bill's alignments with other legislative imperatives. It is likely that there will be further amendments to the Bill as the deliberations of the Parliamentary Portfolio Committee are ongoing. However the "Conditions Governing the Lawful Processing of Personal Information" which are established in Chapter 3 of the Bill are based on international principles and are unlikely to be materially amended. While this guideline will need to be updated in due course once the Bill has been enacted, it is these provisions that are central to attorneys preparing for the enactment of the legislation.

At the time of finalising this Guideline the status of the Bill is that the technical sub-committee appointed by the Parliamentary Portfolio Committee has indicated that the Bill will be enacted in 2011. This guideline is based on the working draft of the Bill published on the 24th February 2011 will be updated to deal with the further amendments in due course. This Guideline should be read in conjunction with Guideline: Information Security for South African Attorneys. This provides guidance to attorneys in managing and securing information which is fundamental to the lawful processing of personal information.

Copyright

Chapter 1

1. INTRODUCTION

1.1 The right of privacy is enshrined in the South African Constitution which expressly states that everyone has the right to privacy[1]. The proposed legislation contained in the Protection of Personal Information Bill is aimed at facilitating the protection of this important right.

1.2 The question of why privacy is important has been addressed in many varying ways. Alan Grayling, one of the foremost contemporary philosophers in the United Kingdom, makes the following observations:

> *"No human rights convention is complete without an article that defends privacy, for the excellent reason that privacy is an indispensible adjunct of the minimum that individuals require for a chance to build good lives. One aspect of its importance is that it gives people a measure of control over the front they offer to others, and the amount of information that others have about them, concerning matters that are personal, intimate, eccentric or constitutive of the individual's inner life. . .*
>
> *But the foremost reason for privacy is that it is crucial for personal autonomy and psychological wellbeing. Even lovers require a degree of privacy from each other, for the lack of a reserve selfhood is almost the same as not having a self at all."*[2]

Grayling's observations highlight the human rights background on which privacy is based.

1.3 Justice Michael Kirby, a renowned Australian judge, who was appointed the chairperson of the OECD Committee which investigated issues of privacy and provided a set of principles for the processing of personal information stated:

> *"There are two visions for the future here. One defends individual privacy, the other gives up ... Resolving these debates presents one of the greatest questions before humanity in this century ... What is at stake is nothing less than the future of the human condition."*

1.4 The dangers of invading a person's privacy and the abuse of personal information has been recognised in countries around the world, many of which have established legislation to address the abuses which are recognised. In Europe, the European Union countries which base their privacy law on a human rights foundation have developed relatively mature legislation and regulation governing the processing of personal information. The Organisation for Economic Cooperation and Development (OECD) (upon which many privacy or protection of personal information regimes internationally are based) have developed principles more from a commercial perspective. Importantly the principles developed with these different backgrounds are largely consistent and overlap with one another.

1.5 The South African Law Reform Commission has thoroughly investigated the development of privacy law globally and chosen to recommend to Parliament a Bill based largely on the principles recognised in the European Union and those of the OECD. Thus the principles reflect already established information security regimes and are in harmony with the protection of personal information initiatives globally.

[1] Section 14 of the Constitution of the Republic of South Africa 1996

[2] Chapter 14 Privacy – Liberty in the Age of Terror (A.C. Grayling)

1.6 Attorneys, by the nature of their practices, typically process vast amounts of personal information. Along with their professional duties of client confidentiality and the more limited but critically important attorney and client privilege requirements, the importance of properly protecting personal information entrusted to attorneys cannot be underestimated.

Chapter 2

2. DEFINITIONS AND ABBREVIATIONS

The aim of this chapter is to assist a reader's understanding of:

- Some of the definitions used in the Bill and in this guideline;
- Abbreviations used in this Guideline.

Definitions

2.1 The definitions are provided to assist the reader of this Guideline and are not the detailed provisions provided in the Bill. Where necessary, regard should be had to the full definition as set out in Section 1 of the Bill.

- "Bill" means the Protection of Personal Information Bill 2009 recommended by the South African Law Reform Commission to the Minister of Justice and Constitutional Development, currently being reviewed by the Parliamentary Portfolio Committee of that Department;
- "Constitution" means the Constitution of the Republic of South Africa 1996;
- "data subject" means the person to whom personal information relates;
- "GAISP" means Generally Accepted Information Security Practices;
- "operator" means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;
- "personal information" means information relating to a person and includes all information about that person, including their characteristics and identifying information and correspondence that are implicitly or explicitly of a private or confidential nature. (The definition provided in the Bill is wide and requires careful consideration.)
- "principles" means the Information Protection Principles articulated in Chapter 3 of the Bill and derived from international privacy instruments;
- "process" means any operational activity concerning personal information including the collection, organisation, storage, modification, communication and destruction of information. (The definition in the Bill is wide and is intended to cover all manner of processing.)
- "record" means any recorded information in whatever form in possession or under the control of the responsible party. (The definition provided in the Bill is wide. The intention is to include all personal information retained in any media.)
- "Regulator" means the Information Protection Regulator as defined in the Bill;
- "responsible party" means a person who determines the purpose of and means of processing personal information (typically, but not always, the collector of information).

[Section 1]

Abbreviations

- "CPA" means the Consumer Protection Act No. 24 of 2009;
- "ECTA" means the Electronic Communications and Transactions Act No. 25 of 2002;

- "FICA" means the Financial Intelligence Centre Act No. 38 of 2001 as amended by the Financial Intelligence Centre Amendment Act No. 11 of 2008
- "ICT" means information and communications technology;
- "NCA" means the National Credit Act NO. 34 of 2005;
- "PAIA" means the Promotion of Access to Information Act No. 2 of 2000;
- "POPIA" means the Protection of Personal Information Bill (recommended by the South African Law Reform Commission and currently being deliberated upon by the Parliamentary Portfolio Committee for Justice and Constitutional Development) which it is contemplated will be enacted into legislation in the near future;
- "PPC" means the Parliamentary Portfolio Committee of the Department of Justice and Constitutional Development;
- "RICA" means the Regulation of interception of Communications Act No. 70 of 2002;
- "SAHRC" means the South African Human Rights Commission;
- "SALRC" means the South African Law Reform Commission.

Chapter 3

3. **APPLICATION OF POPIA**

The aim of this chapter is to inform the reader:

- To what personal information POPIA applies; and
- What information is excluded from the application of POPIA.

Application

3.1 Chapter 2 of POPIA applies to processing of personal information in any form by a responsible party (the person who alone or in conjunction with others, determines the purpose of and means for processing personal information) who or which is domiciled in South Africa, **unless the processing relates only to the forwarding of personal information.**

3.2 Personal information which is processed by non-automated means (eg. paper and text, photographs, x-rays etc.) fall under the ambit of POPIA **only** if they form part of a filing system or are intended to be part of a filing system.

3.3 POPIA applies to both public and private bodies.

Exclusions

3.4 Excluded from the application of POPIA is the processing of personal information:

- For purely personal or household activity;
- Information that has been de-identified;
- Information processed on behalf of the State for the purposes of national security, defence or public safety;
- Information processed for the purpose of investigation and prosecution of criminal matters.

3.5 It is important to note that the exclusions referred to in the last two bullets are only granted to the State if adequate safeguards have been established in the legislation permitting the processing of such information.

3.6 Further exclusions include:

- For exclusively journalistic purposes, provided that the journalists are subject to codes of ethics and adequate standards;[3]
- By the cabinet, the executive council of a province and municipal councils of a municipality;[4]
- The judicial functions of courts; and

[3] This exclusion has been challenged and is subject to a debate in the PPC.

[4] It seems from debates in the PPC that this exclusion will not extend to municipal councils.

- Those exemptions granted by the Regulator in terms of Section 34 of POPIA.

3.7 In instances where other legislation provides safeguards for the protection of personal information that are more extensive than those set out in the information protection principles the more extensive safeguards will prevail.

Chapter 4

4. CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

The aim of this Chapter is to assist attorneys:

- In addressing the lawful processing of personal information; and
- In understanding the 8 conditions which govern the processing of personal information.

Conditions and Principles

4.1 While globally reference to the Conditions referred to in this Guideline are referred to as Principles, in its deliberations, the PPC has required an amendment to Chapter 3 to refer to the Principles as Conditions. Thus, once enacted, Chapter 3 will deal with the "Conditions for Lawful Processing of Personal Information". For the purposes of consistency this Guideline refers to Conditions when dealing with the Bill and Principles when dealing with the Council of Europe, European Union Directive and the OECD Guidelines.

Development of Privacy (Protection of Personal Information) Law

4.2 The conditions contained in Chapter 3 of POPIA derive from the evolution of principles, particularly those developed by the Council of Europe ("CoE") and published in the "Convention for the Protection of Individuals", the European Union directives enacted to support the Convention, as well as the guidelines on the "Protection of Privacy and Trans-border Flows of Personal Data" developed by the Organisation of Economic Co-operation and Development ("OECD Guidelines").

4.3 While deriving from differing philosophies the guidelines provided by both the CoE and OECD cover the protection of personal information and supplement one another. The approaches of the CoE and OECD differed, but it is remarkable how closely the principles developed by these two bodies, using vastly different approaches, overlap. However, one of the fundamental differences in approach adopted by the European Union and followed in the recommendations made by the SALRC has been its requirement for the establishment of an agency to promote, monitor and enforce the protection of personal information.

4.4 The SALRC has recommended to Parliament Protection of Personal Information principles which are derived from both the European Union and the OECD models. It has also recommended the oversight by a Regulator, as required by the European Union model, is implemented in South Africa. This recommendation has been accepted by the PPC and a Regulator will be established to supervise the processing of personal information in compliance with POPIA. The powers of the Regulator currently remain under discussion by the Parliamentary Portfolio Committee. These will be important in the future but for the purposes of this guideline, which deals predominantly with what responsible parties and operators are required to do to comply with the Act, this is not immediately important.

Approach to the Conditions

4.5 It is important to understand that the Conditions do not stand in isolation. They constitute a constellation of Conditions which interact with one another, sometimes overlapping and sometimes complementing and supplementing one another, which need to be applied holistically.

Conditions for Lawful Processing of Personal Information

Condition 1

Accountability

Responsible party to give effect to the principles

"The responsible party must ensure that the conditions set out in this Chapter and all measures that give effect to the conditions are complied with."

[Section 7]

4.6 POPIA mandates that a responsible party, being a public or private body or any other person, who alone or in conjunction with others, determines the purpose of the means of processing personal information, must ensure that the conditions set out in Chapter 3 of POPIA and all the measures that give effect to the conditions are complied with.

4.7 The clear implication of Accountability is that the responsible party remains responsible for the processing of information regardless of it having passed that personal information to a third party (defined as an "Operator"), to process the personal information.

4.8 To enable any responsible person to exercise the control over personal information required by this Condition two critical control measures need to be established and maintained:

- The personal information being processed by a responsible party needs to be identified; and
- The responsible party must identify and appoint a person (or persons) charged with the safeguarding of personal information.

4.9 With regard to the latter of the two control measures, POPIA provides for the appointment of an Information Officer. In the case of a public body an Information Officer means a person contemplated in Section 1 or 17 of PAIA and in the case of a private body, the head of a private body as contemplated in Section 1 of PAIA. In these instances the duties of the Information Protection Officer may be delegated by the head of the public body or private body.

[Section 1]

4.10 The duties and responsibilities of an Information Protection Officer are defined in general terms in POPIA.

[Sections 48 and 49]

4.11 There is a strong overlap between the role of the Information Officer contemplated in POPIA. It is suggested that unless there are compelling reasons for a separation of this duty that responsible parties appoint the same person to fulfil both these roles.

4.12 It must be stressed that while vast bodies of our information are in electronic form and that those people responsible for information technology play an important role in providing the tools to manage and safeguard information, the protection of information and the provision of access to information are business issues. The responsibility for the protection and provision of access to information vests directly with executive controlling bodies, boards and senior executive management. Information is a business issue and should not be delegated or abdicated to people responsible for information technology if they are neither the owners of information nor able to assess the importance of the information.

4.13 Attorneys should note the general responsibility in terms of the new Companies Act that directors of a board must perform the functions assigned to them in good faith and for proper purpose, in the best interests of the company and with a degree of care, skill and diligence that may reasonably be expected of a person carrying out those functions.[5] In addition the director or person carrying out the function must take reasonably diligent steps to become informed of what is necessary to fulfil the function. With specific regard to personal information the provisions of King III need to be heeded. While there is a general duty on any company to protect its business information properly, King III expressly places the responsibility for ICT governance with the board and management of a company. It stipulates that a board should operate with ICT governance in mind and ensure that ICT is a board agenda item.[6] Included in ICT governance is an obligation to ensure appropriate information management, information security, and information privacy. King III recognises these as essential in ensuring appropriate governance of information by organisations that are required to establish appropriate ICT governance.

4.14 In light of the above paragraph attorneys when acting in their capacity as a responsible party should designate a person/s and properly empower the designated person or persons to manage and safeguard its information including personal information for which it is responsible as well as third party information which it may process as an operator on behalf of a third party.

4.15 Thus, on the basis of generally accepted information management security principles, a responsible party should designate and properly empower the designated person or persons to manage and safeguard its information, including its personal information or personal information in its custody. In order to safeguard this information it is critical that an organisation establishes an appropriate information security management system. This must provide for the establishment of an organisational infrastructure, the identification of the organisation's information assets, a risk management methodology defining how the risk relating to an organisation's information assets is to be determined, the development of appropriate policies, processes and standards governing the use of information within the organisation, and mechanisms for the continuous and ongoing review of the organisation's information management and security. Attorneys are referred to the LSSA Guideline Information Security for South African Law Firms.

4.16 Only if this is properly and effectively done will responsible parties and the information officers appointed by responsible parties be able to fulfil their statutory duties and responsibilities and ensure compliance with the information protection principles that are at the heart of the protection of personal information.

[5] Section 76(3) of the Companies Act No. 71 of 2008

[6] Section 111 of the Code of Governance Principles for South Africa 2009

4.17 For responsible parties who have already established an information security management system the wisdom of incorporating the function of information officers within the information security management framework is obvious. However, the specific obligations that are required to be complied with in terms of POPIA should be carefully reviewed and the responsible party must be satisfied that its current structures and management processes accommodate these obligations.

4.18 In those instances where information officers have been appointed by responsible parties to fulfil obligations in terms of the PAIA, responsible parties should review the functional duties of the information officer to ensure that they are properly aligned with the requirements of POPIA. As a matter of experience, in reviewing several organizations' responses to information security and their obligations in terms of PAIA, a striking feature has been that the information security officer or information officer is very often a person ill-qualified for the position.

Condition 2

Processing limitation

Lawfulness of processing

"Personal information must be processed –

(a) lawfully; and

(b) in a reasonable manner that does not infringe the privacy of the data subject."

[Section 8]

4.19 The Processing Limitation condition embraces and underlines the other Conditions of personal information protection. The element of "lawfulness" is fairly straight forward and the responsible party cannot act unlawfully in its collection or processing of personal information.

4.20 The second element of "reasonableness" is perhaps not as straight forward. The notion of fairness incorporates the requirements of balance and proportionality. Responsible parties must therefore take into account the interests and reasonable expectations of data subjects as well as all of the provisions which are incorporated in these conditions. In most instances the foundation for this determination will be the "Purpose Specification" contained in Condition 3, which in turn will inform the data subject's expectation.

Minimality

"Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive."

[Section 9]

4.21 This condition is closely linked to the purpose for which information may be processed. It is intended to ensure that only personal information which is appropriate for the purpose it is being collected, is collected. It should also be noted that it also relates to the nature of the processing which is being contemplated. In those circumstances where a data subject's consent to processing is obtained, it is

likely to be viewed in a more relaxed light than where the processing of personal information is used legitimately but without the consent of the data subject.

Consent, Justification and Objection

[Section 10]

4.22 **Consent** is an important element in the mechanics of processing personal information but it is not the sole element.

[Section 10(1)(a)]

4.23 POPIA defines consent as meaning "voluntary, specific and informed expression of will in terms of which a data subject agrees to the processing of personal information relating to him or her."[7] It is also submitted that although the word "unambiguous" is not used in the wording of POPIA that the consent must be unambiguous.

4.24 All of the normal principles relating to voluntary consent would also apply. The consent must be voluntary and must not amount to a submission. Thus principles which govern unilateral consent in our law would apply equally in the interpretation of consent in this context.

4.25 It is worth noting that there is no provision which requires that the consent of the data subject needs to be in writing. In the circumstances if a data subject is offered an opportunity to object to the use of personal information and fails to do so, consent may be inferred from this omission. It is also important to note that consent relating to the use of personal information revocable by the data subject at any time.

4.26 Processing is lawful and **justifiable** if it carried out in terms of the provisions of paragraphs 10(1)(b) to (f). Thus it must be stressed that POPIA is not "consent" driven. This is clear from the provisions of Section 10(1)(b) to (f) which provide for the processing of information without the consent of the data subject but for the specific purposes that include:

- The processing is necessary in terms of a contract to which the data subject is a party;
- Processing complies with law;
- Processing which protects a legitimate interest of a data subject;
- Processing is necessary to fulfil a public law duty;
- Processing is necessary for the legitimate interests of a responsible party or third party to whom information is supplied.

[Sub-Section 10(1)(b) to (f)]

4.27 **A data subject may object**, at any time, on reasonable grounds to the processing of personal information and if the data subject has objected, the responsible party must immediately stop processing the data subject's personal information.

[Sections 10(2) and (3)]

[7] Section 1 of POPIA

Collection directly from data subject

4.28 Subject to the exceptions set out below the responsible party must collect personal information directly from a data subject.

[Section 11(1)]

4.29 At first blush and without the exceptions which are discussed below, this provision may seem to be very strict. However, the exceptions are extensive and the impact of this provision is considerably softened by the application of the exceptions.

4.30 The condition is intended to promote the principle that the data subject has knowledge of information which is being collected by a responsible party. The section should also be read together with the "Purpose Specification Condition" and in particular Section 13, which requires that steps must be taken to ensure that the data subject is aware of the purpose of the collection of information by the responsible party. Thus, even where information is collected from a third party, the data subject should be made aware of the processing of the information and the purpose for which the information has been collected. Clearly in certain instances this would not apply but it would be incumbent on the responsible party to show that it was not possible to collect the information directly from the data subject and that the responsible party was justified in not making the data subject aware of the purpose for which the information was collected.

4.31 The responsible party is not obliged to collect personal information directly from the data subject if:

- The information is contained in a public record or has deliberately been made public by the data subject;
- The data subject has consented to the collection of the information from another source;
- The legitimate interests of the data subject are not prejudiced;
- Collection from another source is necessary to avoid the prejudice of the maintenance of law, the enforcement of law, the collection of revenue by SARS, conduct of court proceedings, the legitimate interests of national security or the maintenance of legitimate interests of a responsible party;
- Compliance would be prejudicial to a lawful purpose; or
- Compliance is not reasonably practicable.

[Section 11(2)]

4.32 In certain instances which are established in these exceptions, the collection of personal information from a data subject would defeat the legitimate purpose of the collection of the information. For instance the purpose of the collection of information relating to criminal activities or those of national security would be subverted if the consent of the data subject needed to be obtained.

Condition 3

Purpose specification

4.33 This condition entails three separate elements, the collection for a specific purpose, that the data subject is aware of the purpose of collection and the retention of personal information for no longer than it may be required.

Collection for a Specific Purpose

4.34 POPIA requires that the information must be collected for a specific, explicitly defined and lawful purpose which relates to the activity of the responsible party.

[Section 12]

4.35 The purpose of the collection and processing of personal information influences every aspect of the processing of the information, the manner of its collection, periods of retention, further processing, disclosure to third parties and any further issues which may apply to the processing of the information.[8]

4.36 It should also be noted that while the responsible party will have a duty to notify the Regulator of its purposes and functions, the factor determining the purpose for the collection of personal information will always be the specified purpose communicated to the data subject.

Data Subject Aware of the Purpose and Collection of Information

4.37 The responsible party must ensure, in collecting the information, that the data subject is aware of the purpose for which the information is being collected. This enables the data subject to make an informed decision as to whether the personal information should be made available to the responsible party. In this regard it is clear that the data subject must be informed before the collection and processing of the personal information. In considering how the data subject must be made aware of the purpose of collection regard should also be had to the "Openness" Condition and Section 17(2) of the Act which stipulates the reasonable steps that a responsible party should take in ensuring that the data subject is aware of the purpose of the collection and processing of the information.

[Section 13]

Retention of records

4.38 In terms of the Purpose Specification condition it is also important that records are not retained for any longer than is necessary for achieving the purpose for which the information was collected or processed. There are exceptions to the retention requirement which need to be carefully considered in determining retention periods and when personal information is to be destroyed.

[Section 14]

4.39 Record retention is a subject which does not receive the consideration it deserves in most businesses. While information was only in paper and text we developed good record retention methodologies

[8] "Information and Communications Technology Law" at page 374 (Chapter 8 : Data Protection Protection, Professor A. Roos)

appropriate to the physical nature of the records. However, it is submitted that record retention in organisations, which now rely predominantly on electronic information, generally leaves much to be desired. Most organisations do not identify and categorise records which are retained or, who is responsible for ensuring that the retained records are appropriately safeguarded. The result is that in most organisations different versions of the same record may exist, be held by different persons and be subject to different degrees of security safeguard.

4.40 In the circumstances, in order to comply with the provisions of Section 14, record retention generally and more specifically retention of records containing personal information, demands careful consideration.

Condition 4

Further processing limitation

4.41 The further processing of any personal information must be compatible with the purpose for which it was initially collected.

[Section 15]

4.42 By way of example, if a party collects information for the purposes of opening a cheque account, the information cannot then be further processed to market insurance. This is so even if the responsible party may provide both facilities.

4.43 To assist in determining whether further processing is compatible with the initial purpose of collection, a responsible party must take account of:

- The relationship between the purpose for which the information was originally collected and the intended purpose of any further processing;
- The nature of the information concerned;
- The consequences of further processing;
- The manner in which the information was collected; and
- Contractual rights and obligations between the parties.

4.44 The Condition establishes instances where further processing not compatible with the purpose of its initial collection, is necessitated by overriding public interest, or is allowed by the Regulator.

Condition 5

Information quality

Quality of information

4.45 The Information Quality condition requires that the responsible party take reasonably practicable steps to ensure that information is complete, accurate, not misleading and, where necessary, is updated.

[Section 16]

4.46 In essence this condition requires that appropriate information security measures safeguarding the integrity of the personal information be employed. This is an information security principle which needs to be taken into account in considering compliance with the ECTA. Chapter 3 of that Act explicitly requires that the integrity, reliability and accuracy of electronic information be maintained if they are to enjoy the efficacy that the ECTA bestows on them. The same principles that need to be employed in protecting the integrity of information and its updating apply equally in this instance. It is also interesting to note that in dealing with IT governance King III requires that information security must be established and maintained if the obligation to properly govern IT and information is to be discharged.[9]

Condition 6

Openness

Notification to Regulator and to data subject

4.47 The purpose of this condition is to ensure transparency and fairness in the processing of personal information.

[Section 17]

4.48 The first obligation is that a responsible party must notify the Regulator before personal information may be processed by the responsible party. If the responsible party has compiled a manual in terms of PAIA and has published it (typically by making it available on its website and providing a copy to the SAHRC) it does not have to comply with the notification to the Regulator.

4.49 The second obligation is providing the data subject with information which allows the data subject to be aware that personal information is being collected, the identity of the responsible party, the purpose for the collection of the information and whether the supply of the information by the data subject is voluntary or mandatory.

4.50 Exceptions to compliance with the Openness condition are provided for. These include consent of the data subject to non-compliance, processing if the data subject is not identifiable and in certain instances, public and security interests.

Condition 7

Security Safeguards

Security measures on integrity of personal information

4.51 The Security Safeguards condition underlines the obligation of the responsible party to ensure that personal information of a data subject in its possession or under its control is appropriately safeguarded against loss, destruction or unlawful access.

[9] Principle 5.6 (35) and 5.6 (40) of King III

[Section 18]

4.52 The use of the word "Protection" in the name of POPIA immediately identifies the necessity for ensuring security safeguards for personal information. As has already been stated in this guideline, information security standards have developed and are now recognised as international standards, which address the security of information generally and may be applied to address the security of personal information. These standards (and Generally Accepted Information Security Practices based on these Standards) assist in determining what security technologies are appropriate, how policies should be developed and people educated in the policies to achieve the ultimate goal of information security. This will assist organisations in protecting information (including personal information) against unauthorised access or alteration and ensuring the availability of accurate information to authorised persons when it is required. Due to the importance of information security in dealing with the protection of personal information, the disciplines of information security must be established within an organisation and the practical measures that need to be taken by the organisation in safeguarding its information and personal information must receive the appropriate priority and attention. Attorneys are referred to the LSSA Guideline Information Security for South African Law Firms.

Information processed by operator or person acting under authority of a responsible party

4.53 Any third party or operator processing personal information for the responsible party must do so only with the knowledge and express authorisation of the responsible party and must treat the personal information as confidential.

4.54 In line with the responsible party's obligations to the data subject, the responsible party always has the obligation to ensure that an operator processing information on its behalf establishes security safeguards and that these measures are maintained. The processing of personal information and the security safeguards required by the responsible party should be governed by written agreements. The responsible party is also obliged to ensure that an operator not domiciled in the Republic, adheres to the laws governing the processing of personal information.

[Sections 19 and 20]

Notification of security compromises

4.55 A responsible party must, in instances where personal information has been compromised, notify the Regulator and the data subject, unless the identity of the data subject cannot be established.

[Section 21]

4.56 The duty to notify a security breach which compromises personal information is relatively novel. First adopted in California and now adopted by in excess of 45 of the States in the United States of America, as well as being the subject of a European Union directive, the principle recognises that the data subject is best able to protect personal information owned by the data subject.

Condition 8

Data subject participation

Access to personal information

4.57 This provision (which is similar to the Request provisions of PAIA) confers on a data subject the right to request a responsible party to confirm, free of charge, whether the responsible party holds personal information about the data subject.

4.58 Further, the data subject may request the responsible party to provide it with a description of the personal information held by it or by a third party within a reasonable time. Any fees charged for providing the data subject with the information required shall not be excessive. The responsible party should also advise the data subject that the personal information may be corrected against request.

[Section 22]

4.59 As these provisions allow for the access to personal information they should be aligned with mechanisms within an organisation dealing with requests for information in terms of PAIA. The Condition expressly provides that Sections 18 and 53 of PAIA apply to requests made in terms of Sections 22 and 23 of POPIA.

Correction of Personal Information

4.60 This provision deals specifically with the right of a data subject to request a correction or deletion of personal data. The provisions of POPIA place a duty on the responsible party to investigate the request and to respond thereto. In those circumstances where the responsible party believes that the information is accurate and no agreement between the data subject and the responsible party can be reached to amend the information, the responsible party is obliged to link the personal information in dispute, in such a manner that it will always be read, with an indication that the correction of the personal information has been requested by the data subject but has not been made.

4.61 In cases where changes have been made which may impact on decisions taken using personal information POPIA imposes a duty on the responsible party to advise, if reasonably practical, any third parties to whom the information may have been disclosed.

[Section 23]

Chapter 5

5. REFERENCES

The aim of this chapter is to provide the attorney with references to publications which may assist in dealing with the protection of personal information and access to information.

South African Law Reform Commission Report to the Minister of Justice and Constitutional Development

5.1 This report documents the research conducted principally by Advocate Ananda Louw the Principal State Law Advisor, and provide a comprehensive cross-referencing of research undertaken by her. It is an excellent guide to references which may be required in research issues relating to the report.

5.2 In addition to the materials provided with this guideline readers are referred to the report of the South African Law Reform Commission (Project 124 Privacy and Data Protection Report 2009). This report may be accessed at **http://www.justice.gov.za/salrc/reports/r_prj124_privacy.pdf**.

The index to the report is:

"Information and Telecommunications Law" published by Lexis Nexis.

5.3 Chapter 8 of this publication deals with data protection. The author of this Chapter, Professor Anneliese Roos, provides a commentary on the Bill which is useful. However, care needs to be taken, in the same manner as in this guideline, as amendments to the Bill prior to its enactment will need to be taken into consideration.

Information Security Commissioners

5.4 There are many websites of Information Security Commissioners which deal with the application of privacy law in a particular jurisdiction which can provide valuable insight into how privacy issues may be dealt with. The reader is referred to the web addresses of the following Commissioners or Regulators which have been established for some time and which provide valuable guidance by way of guidelines and rulings made by the Commissioners or Regulators.

- Information Commissioner's Office England and Wales **www.ico.gov.uk**
- Information Commissioner of Canada **www.infocom.gc.ca**
- Australia's Privacy Commissioner **www.privacy.gov.au**
- Privacy Commissioner New Zealand **www.privacy.org.nz**
- European Commission Justice and Home Affairs: Data Protection **www.ec.europa.eu.justice**. This site provides details to enable access to all European Union personal data protection officers.

Privacy Law United States of America

5.5 There are many websites dealing with privacy rights in the USA but one which appears to be more comprehensive than others is the Privacy Rights Clearing House website which may be found at **www.privacyrights.org**.