LAW SOCIETY
OF SOUTH AFRICA

LSSA GUIDELINES

PROTECTION OF PERSONAL INFORMATION FOR SOUTH AFRICAN LAW FIRMS

Prepared for the Law Society of South Africa by Mark Heyink

LSSA Guidelines

Protection of Personal Information for South African Law Firms

VERSION 4.0

Attorney, Notary & Conveyancer
Specialising in Information Law

Foreword

Please read this foreword carefully.

This guideline is version 4.0 of Protection of Personal Information Guidelines compiled for the Law Society of South Africa. It incorporates references to important developments that have occurred in the realm Protection of Personal Information, or "Data Protection" as this developing jurisprudence is known in some jurisdictions.

The most notable addition to the data protection landscape is the General Data Protection Regulation (GDPR), which will govern Data Protection in all of the European Union member countries. The GDPR will commence on the 25th May 2018 and is regarded as the gold standard in the protection of privacy of information. Democracies around the world are looking to the GDPR to update their own legislation and regulation in an attempt to keep pace with the explosion of processing of information as novel information and communication technologies disrupt and transform our 21st Century world. By way of example, the United Kingdom, having exited from the European Union, has deemed it necessary to promulgate a new Data Protection Act to ensure that it can work in harmony with other EU countries and that it stays at the forefront of data protection.

The revision of this guideline addresses the potential impact of GDPR on South African companies. It is also highly likely that where the Information Regulator ("Regulator") is required to interpret the Protection of Personal Information Act (PoPIA, as the Regulator prefers it to be referred to) it will seek guidance in interpretations contained in the GDPR, particularly where they relate to novel practices not necessarily addressed in PoPIA. This is in line with the constitutional imperative contained in Section 233 of the Constitution and Constitutional Court pronouncements to the effect that relevant international law is considered in interpreting areas of uncertainty in South African law.

The primary purpose of the guideline as is to assist attorneys in familiarising themselves with their obligations to lawfully process personal information in their practices. 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.

This Guideline should be read in conjunction with the "Guideline: Information Security for South African Law Firms". 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]. PoPIA 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 indispensable 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 danger 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 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 are based globally) have developed principles more from a commercial perspective. Importantly the principles developed with these different backgrounds are largely consistent and overlap one another.

1.5 The South African Law Reform Commission thoroughly investigated the development of privacy law globally and chosen to recommend to Parliament legislation based largely on the principles recognised in the European Union and those of the OECD. Thus, the principles incorporated into

[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)

PoPIA reflect already established information security regimes and are in harmony with the protection of personal information initiatives globally.

1.6 PoPIA was long in gestation. The Parliamentary Portfolio Committee of the Department of Justice and Constitutional Development appointed a sub-committee to deal with the issues and approach recommended by the SALRC, which in many respects were novel to South Africa. To the great credit of the representatives of the parties, party politics were to a large degree set aside in crafting the legislation. True to its purpose of protecting the right of privacy, including the right of protection of personal information cognizant of constitutional values, PoPIA is in harmony with developing international standards and balances the rights of Protection of Personal Information against other legislative and constitutional rights, in particular the right of access to information.

1.7 Regrettably, since its enactment on the 26th November 2013, now some 4 years ago, the Department of Justice has, at best, been tardy in advancing the implementation of the Act. There have been numerous delays, the most significant and obvious of which has been the delay in the appointment of the Information Regulator. The Information Regulator was only appointed in 2016 and is not yet in a position to recommend to the State President that he can proclaim the commencement of the Act.

1.8 The Information Regulator is an independent regulatory body in line with jurisdictions that have proved most successful in governance of the protection of personal information. Its powers, duties and functions include:

- Education, including the promotion of understanding and acceptance of the Conditions of Lawful Processing of Personal Information;
- Monitoring and enforcement of compliance through the powers vested in it by the legislation;
- Consultation with interested parties on a national and international basis;
- The handling and investigation of complaints;
- Conduct of research and reporting to Parliament on international developments;
- Addressing the protection of personal information;
- The establishment and development of codes of conduct;
- Facilitation of cross-border cooperation with other jurisdictions; and
- Generally establishing and nurturing a culture which protects personal information in South Africa.

1.9 One of the negative aspects of the delays has been that the elsewhere the jurisprudence relating to the Protection of Personal Information has developed quickly in an attempt to keep pace with the explosive changes that the advent and use of modern technologies have brought to our society, economies and indeed even to our political landscape. Thus, while significant progress has been made in democracies around the world, since 2011 when the wording of PoPIA was finalised not only have the delays in the implementation of PoPIA had an adverse effect on South Africans and the protection of the constitutional right of privacy, but it has also seen South Africa fall behind other democracies, to the extent that our law and particularly the failure to implement the law properly may render South Africa one of the countries whose law may not be adequate in the eyes of European countries once the GDPR has commenced.

1.10 In the United States of America privacy to a large degree, save for specific sectoral legislation, has been governed at State level but it is recognised that this is no longer tenable and a far more consistent and harmonised approach, in line with international developments, has to be adopted. The importance placed on privacy in this regard is reflected in the following statements made by President Obama in addressing Congress and the American people:

> *"Never has privacy been more important than today, the age of the Internet, the world wide web and smart phones. In the last decade, the Internet has enabled a renewal of direct political engagement by citizens around the globe and an explosion of commerce and innovation creating jobs of the future. Much of this innovation is enabled by novel uses of personal information. So, it is incumbent on us to do what we have done throughout history: Apply our timeless privacy values to the new technologies and circumstances of our times. . . .*
>
> *One thing should be clear, even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value. It has been at the heart of our democracy from its inception, and we need it now more than ever."*

1.11 The Trump Administration does not regard privacy in the same light as President Obama. After making several campaign statements regarding privacy, President Trump has, however, not repealed or had amended privacy protections that exist in the United Statement of America. It does appear that there is a strong lobby from many of the technology companies in the USA that government policy should become more aligned with the privacy developments in democratic countries. This seems, for the moment at least, to have prevented the Trump Administration from seeking to implement policy unduly favouring national security over personal privacy interests.

1.12 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. In addition, attorneys have an obligation of creating and fostering a culture which promotes and enhances our constitutional values. In the context of privacy, an attorney's obligation is to assist citizens in ensuring that their right of privacy is protected by third parties processing their information and that they can enforce their rights against those third parties who failed to do so.

1.13 The attention of attorneys is also drawn to the fact that the Information Regulator has published draft Regulations. Comment has been received on the draft Regulations that were published but there is no indication at this stage when the Regulations will be finalised for submission to the Minister for publication. These will provide some guidance as to how the Protection of Personal Information and interaction with the Information Regulator will be administered. Attorneys are urged to familiarise themselves with the Regulations as soon as these are published.

Chapter 2

2. DEFINITIONS AND ABBREVIATIONS

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

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

PoPIA Definitions

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

- "Act" means the Protection of Personal Information Act No. 4 of 2013;
- "Conditions" means the Conditions of Lawful Processing stipulated in Chapter 3 of the Act, unless the context indicates a contrary meaning;
- "Constitution" means the Constitution of the Republic of South Africa 1996;
- "data subject" means the person to whom personal information relates;
- "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 PoPIA is wide and requires careful consideration.)
- "principles" means information protection principles articulated in Privacy Guidelines, from which the Act has been developed, including without limitation, the European Union Directive (1995) and the OECD Privacy Guidelines (Attention is drawn to Chapter II of the GDPR which refers to "principles" that are materially similar to the conditions for lawful processing stipulated in PoPIA);
- "processing" means any operational activity concerning personal information including the collection, organisation, storage, modification, communication and destruction of information. (the definition in PoPIA 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 PoPIA is wide. The intention is to include all personal information retained in any media.)
- "Regulator" means the Information Regulator established in terms of the Act;
- "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
- "GAISP" means generally accepted information security practices that have been accepted as guidelines or standards governing the implementation of frameworks and control measures intended to facilitate the security of information. (eg. The ISO27000 suite of Standards published by the International Standards Organisation);
- "GDPR" means the General Data Protection Regulation (EU) 2016/679 of the European Parliament dated the 27th April 2016;
- "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 Act No. 4 of 2013 (in this Guideline the abbreviation is used interchangeably with the "Act");
- "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.

GDPR Terminology

2.2 The GDPR is important to how we consider the Act as the Information Regulator is likely to take cognisance of the GDPR in its interpretation of the Act. The GDPR is referred to in this guideline and to facilitate the ease of understanding attention is draw to the following the following differences in terminology.

- Where the GDPR refers to "articles" PoPIA refers to "sections";
- Where the GDPR refers to "controller" PoPIA refers to "responsible party";
- Where the GDPR refers to "processor" PoPIA refers to "operator";
- Where the GDPR refers to "supervisory authority" PoPIA refers to "the Information Regulator". The term "supervisory authority" refers to a National Supervisory Authority.

Chapter 3

3. PURPOSE, APPLICATION AND EXCLUSION

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

- The application and interpretation of the Act;
- To what personal information the Act applies; and
- What processing of personal information is excluded from the application of the Act.

Purpose

3.1 The purpose of the Act is to:

- give effect to the constitutional right of privacy, in particular the safeguarding of personal information subject to justifiable limitations aimed at balancing the right of privacy against other rights, particularly that of access to information protecting the free flow of information;
- regulate the processing of personal information in harmony with international standards3;
- prescribe minimum requirements for the lawful processing of personal information;
- provide rights and remedies to protect against abuses of personal information; and
- establish a Regulator to promote, enforce and fulfil the rights protected by the Act.

3.2 The Act also addresses the use of personal information in direct marketing by way of unsolicited electronic communication, the restrictions on trans-border information flows and protects the personal information of children. These are all burning issues in our information age which are being dealt with in jurisdictions across the globe.

[Section 2]

Application

3.3 Chapter 2 of the Act 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 or if not domiciled in South Africa, makes use of automated or non-automated means in South Africa, **unless the processing relates only to the forwarding of personal information through South Africa.**

3.4 Personal information which is processed by non-automated means (eg. paper and text, photographs, x-rays etc.) falls under the ambit of the Act **only** if it forms part of a filing system or is intended to be part of a filing system.

[3] While international standards are wider than the GDPR, fundamentally the GDPR, as it affects the whole of Europe and is the most advanced statutory instrument on the Protection of Personal Information is likely to prove the most important standard in the South African context. It would be wise to recognise that PoPIA, based, as it is, on prior EU standards and that the principles adopted by the EU, will inevitably be strongly influenced by the GDPR.

3.5 the Act applies to both public and private bodies.

[Section 3]

Exclusions

3.6 The Act will not apply to the processing of personal information:

- for purely personal or household activity;
- that has been de-identified;
- processed by or on behalf of a public body for the purposes of:
  - safeguarding national security
  - the investigation and prosecution of criminal matters
  - processed by the cabinet and its committees or the executive council of a province; or
  - relating to the judicial functions of a court.

3.7 The exclusions are subject to the proviso that adequate safeguards are established in legislation involving national security and lawful activities that properly protect personal information.

3.8 The exclusions referred to in 3.6 relating to processing by or on behalf of a public body for the purposes of national security and the investigation of crime, do not free any organ of State from providing adequate safeguards to ensure that the controls contemplated in the Act that do not influence national security or the investigation of crime are established and maintained.

[Sections 6]

GDPR

3.9 It is important to note that the GDPR is limited to the protection of natural persons and not to juristic persons as is the case with PoPIA.

3.10 The GDPR expressly states that the protection of personal data is a fundamental right and refers to the Charter of Fundamental Rights of the European Union and the treaty on the functioning of the European Union in this regard. Several of the European Union members do not have a constitution or a Bill of Rights. In the South African context, the right of privacy is expressly protected in the Bill of Rights section of the Constitution. This is important in considering the balancing of rights against one another and the legitimate interests of data subjects on the one hand and persons processing the data subject's personal information on the other.

3.11 The GDPR also allows for the application of member state laws where these are applicable. This is of particular importance relating to national security and criminal investigation and prosecution. In these instances member state laws will take precedence over the GDPR.

ePrivacy Regulation

3.12 It is important to be aware of the EU proposal concerning the respect for private life and the Protection of Personal Information in electronic communications that is currently being considered by the European Parliament (this is termed the ePrivacy Regulation.) This may have significant impact on various aspects of PoPIA in the future.

3.13 While it may be important to carefully consider the differences between PoPIA and the GDPR in wishing to apply aspects of the GDPR in the interpretation of PoPIA, it is true that the purpose and scope of both instruments are closely aligned.

3.14 The Act further provides that the Act does not apply to:

- the processing of personal information for the purposes of journalistic, literary or artistic expression in defined circumstances;
- the exclusion for journalistic purposes requires the journalist to be subject to a code of ethics and provides adequate safeguards for the protection of personal information.

[Section 7]

3.15 The Regulator may grant exemptions to compliance with the Conditions for the Lawful Processing of Personal Information.

Chapter 4

4. CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

The aim of this chapter is to assist the reader:

- 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 the Conditions referred to in this Guideline are referred to as "Principles", in its deliberations, the PPC required an amendment to Chapter 3 to refer to the Principles as Conditions. Thus, Chapter 3 addresses the "Conditions for Lawful Processing of Personal Information".

4.2 The GDPR refers to "Principles relating to the processing of personal data".

4.3 For the purposes of consistency this Guideline refers to "Conditions" when dealing with PoPIA and "Principles" when dealing with the GDPR and the OECD Guidelines.

Development of Privacy (Protection of Personal Information) Law

4.4 The conditions contained in Chapter 3 of the Act 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").

4.5 From the 25th May 2018 the GDPR will replace the European Union Directives referred to in 4.4.

4.6 While deriving from differing philosophies the guidelines provided by the CoE and OECD both 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. This agency is referred to as the Regulator in the Act.

4.7 The GDPR expressly requires that each member state must establish an independent supervisory authority. The GDPR allows for more than one supervisory body but provides that each member state must designate a particular supervisory authority to represent a country in contributing to a consistent approach to data protection throughout the European Union.

Approach to the Conditions

4.8 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. It is therefore necessary to consider the conditions holistically and it is also recommended that where there may be perceived contradictions that regard be had to co-relative articles in the GDPR and the comment that is provided in the Recital contained in the GDPR prior to the articles. This will often be helpful in providing context and information gained in the more mature experience of the Europeans in protecting personal information.

Conditions for Lawful Processing of Personal Information

Condition 1

Accountability

Responsible Party to Ensure Conditions for Lawful Processing

"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 8]

4.9 The Act 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 the Act and all the measures that give effect to the conditions are complied with.

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

4.11 To enable a responsible party 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.

4.12 With regard to the latter of the two control measures, the Act 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 alternatively Section 17 of PAIA. In these instances the duties of the Information Officer may be delegated by the head of the public body or private body.

[Sections 1 and 55]

4.13 The duties and responsibilities of an Information Officer are defined in general terms in the Act.[4]

[Sections 55 and 56]

4.14 There is a strong overlap between the role of the Information Officer contemplated in the Act and the role of the person responsible for access to information in terms of PAIA. 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. In many instances these roles may also fruitfully include the duties of an information security officer, being the person responsible for the day to day adherence, monitoring and enforcement of policies, procedures and standards established by an entity in implementing information security management systems. In this regard the reader is referred to the LSSA Guideline: Information Security for South Africa Law Firms.

4.15 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.

4.16 Attorneys should note the general responsibility in terms of the 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 IV expressly places the responsibility for ICT governance with the board and senior management of a company delegated by the board to manage and secure information. 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 IV recognises these as essential in ensuring governance of information by organisations that are required to establish appropriate ICT governance measures.

4.17 In light of the above paragraph when acting in their capacity as a responsible party, attorneys should they choose, must designate a person/s to manage and safeguard information, including personal information for which the attorney may be responsible. They must then properly empower the designated person/s. Similarly, where an attorney processes information, including personal information, as an operator on behalf of a third party, responsibility must be assigned and the person processing the information must be properly empowered to ensure that personal information is protected.

[4] Attention is drawn to the draft Regulations published by the Information Regulator on which comment has been submitted. This sets out in draft Regulation 4 the responsibilities of an Information Officer. It is recommended that care be taken to consider the Regulations once they are published by the Information Regulator and consider the Information Officer's duties in light thereof.

[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

4.18 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. Readers are referred to the LSSA Guideline Information Security for South African Law Firms.

4.19 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.

4.20 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 the Act should be carefully reviewed and the responsible party must be satisfied that its current structures and management processes accommodate these obligations.

4.21 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 the Act. 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 9]

4.22 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 must not act unlawfully in its collection or processing of personal information.

4.23 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.

4.24 The GDPR stipulates that personal data should be processed lawfully, fairly and in a transparent manner in relation to the data subject. This principle is aligned with the concept that the data subject is entitled to know how information is being processed and be in a position to determine whether they are prepared to allow their information to be processed in the manner contemplated and if not, refrain from providing the information, alternatively object to the processing of their information in a manner that would be unfair to them.

4.25 This does not prevent the processing of personal information in circumstances where although it may have an effect on the data subject, its processing remains fair. For example, although the processing of personal information for the purposes of a traffic fine may be adverse to the data subject, its processing is justified and fair.

Minimality

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

[Section 10]

4.26 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.

4.27 The Principle stipulated in the GDPR is materially identical to the Condition of Minimality in PoPIA.

Consent, Justification and Objection

[Section 11]

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

[Section 11(1)(a)]

4.29 The Act defines consent as meaning "any 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 the Act that the consent must be unambiguous.

[7] Section 1 of the Act

4.30 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.

4.31 It is worth noting that there is no provision which requires that the consent of the data subject needs to be in writing. It is submitted, however, that the consent of the data subject must be clear and the onus rests on the responsible party to demonstrate that the data subject has consented. This submission is supported by the definition in the GDPR that goes further than PoPIA in including in the definition the requirement that consent can only be inferred if the data subject "... by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her ...".

4.32 The GDPR in Article 7 also stipulates conditions for consent that place a more restrictive interpretation on consent than may be possible with PoPIA. It is suggested that the Information Regulator may well refer to the GDPR and assert the more restrictive interpretation, particular as this is in line with rapidly evolving efforts to protect the data subject globally.

4.33 It is important to note that the GDPR expressly requires that "It shall be as easy to withdraw as to give consent". This must be taken into consideration in a responsible party's interaction with clients and in processing the personal information.

4.34 Processing is lawful and **justifiable** if it is carried out in terms of the provisions of paragraphs 11(1)(b) to (f). Thus it must be stressed that the Act is not "consent" driven. This is clear from the provisions of Section 11(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 necessary to fulfil a public law duty; and
- processing necessary for the legitimate interests of a responsible party or third party to whom information is supplied.

[Sub-Section 11(1)(b) to (f)]

4.35 The issue of **"Legitimate interest"** has been widely speculated upon by entities within South Africa. Unfortunately, this speculation has typically been based on interpreting legitimate interests to serve the interest of the processor rather than the data subject. This type of self-serving justification is unlikely to find any currency with the Information Regulator and very definitely runs contrary to the provisions of the GDPR.

4.36 In the GDPR the wording relating to the interests of a data subject is different. The GDPR provides that processing is only lawful if "…it is necessary in order to protect the **vital interests** of the data subject or of another natural person". In this regard the Recital contained in paragraph 46 of the GDPR is illuminating. It states "The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential **for the life of the data subject** or that of another natural person". Therefore in determining the balance of interests between that of a processor, (whether they are a responsible party or an operator) and the data subject or another third party, it is only in those instances where the processing is essential to the life of the data subject or the third party that a responsible party will be entitled to process the information.

4.37 With regard to the use of the wording "legitimate interests of a responsible party" it must be borne in mind that the constitutional rights of privacy of a data subject must be taken into account and balanced with the rights of the processor. It is also submitted that the legitimate expectations of the data subject would also need to be taken into account in determining whether the processing is justified.

4.38 The GDPR, in providing the qualification to legitimate interests, states "Except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject which require protection of the personal data ...".

4.39 **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 11(2) and (3)]

Collection directly from data subject

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

[Section 12(1)]

4.41 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.

4.42 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.

4.43 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 12(2)]

4.44 In the 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 example 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.

4.45 The GDPR places emphasis on collection directly from a data subject. This is in view of the fact that the issue of transparency and notice to a data subject of processing is more stringently dealt with. This allows the data subject to know how his or her personal information is being processed and to object to the processing, regardless from where the personal information may have been sourced.

4.46 In view of the fact that South Africa is considerably behind most democratic countries in the implementation of data protection law, it is suggested that the practical issues relating to notification of data subjects will be difficult to overcome. Nonetheless, the Notification provisions in Section 18 of PoPIA deserve considerable attention from processors of personal information who will have to adhere to this provision after the expiry of the grace period following the proclamation of commencement of the Act.

Condition 3

Purpose specification

4.47 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

4.48 The Act 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 13]

4.49 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]

4.50 While initial drafts of PoPIA required notification by Responsible Parties to the Regulator of the Responsible Parties' purposes and functions, this requirement has fallen away. It is no longer necessary to notify the Regulator, save in circumstances where prior authorisation of the Regulator to the processing of personal information is required.

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

Data Subject Aware of the Purpose and Collection of Information

4.51 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.

[Section 13]

Retention of records

4.52 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]

4.53 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 appropriate to the physical nature of the records. It is submitted, however, that record retention in most organisations, which now rely predominantly on electronic information, leaves much to be desired. Most organisations do not categorise records which are retained or, identify 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 differing security safeguards.

4.54 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. If you do not have a proper record retention policy is implemented PoPIA makes it imperative that this is addressed. Even if you do have a good record retention policy, PoPIA probably demands that this be reviewed and, if necessary, revised.

Condition 4

Further processing limitation

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

[Section 15]

4.56 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.

4.57 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.

4.58 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.

4.59 The GDPR in Article 5(1)(b) provides that "Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; …". The processing for archiving purposes, public interest, scientific or historical research purposes or statistical purposes is not considered to be incompatible processing.

Condition 5

Information quality

Quality of information

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

[Section 16]

4.61 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 III 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.

4.62 King IV expressly requires dealing with "Technology and information governance":

> *"14. The governing body should exercise ongoing oversight of the management of information and, in particular oversee its results in the following:*
>
> *a. The leveraging of information to sustain and enhance the organisation's intellectual capital.*
>
> *b. Information architecture that supports confidentiality, integrity and availability of information.*

c. *The protection of privacy of personal information.*

d. *The continued monitoring of security of information."* [9]

Condition 6

Openness

Notification to data subject

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

[Section 17]

4.64 The provisions of Section 14 (applicable to public bodies) and Section 51 (applicable to private bodies) of PAIA form part of the Openness Principle in terms of this Condition.

[Section 17]

4.65 A responsible party is obliged to ensure that the data subject is aware of:

- the information being collected and if not from a data subject, the source from which it is collected.
- The name and address of the responsible party
- The purpose of collection
- Whether the supply of information by the data subject is voluntary or mandatory
- The consequences of failure to provide information
- Law authorising or requiring the collection of information
- If to be transferred to a third country or international organisation, the level of protection afforded to the information
- Any further relevant information

[Section 18]

4.66 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.

[9] King IV Part 5.4: GOVERANCE FUNCTIONAL AREAS Principle 12, paragraph 14

Condition 7

Security Safeguards

Security measures on integrity of personal information

4.67 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.

[Section 19]

4.68 The use of the word "Protection" in the title of the Act 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.

4.69 The GDPR provides in Article 5(1)(f) that "Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).".

4.70 This is one of the few instances where PoPIA is more extensive in describing the obligations of a responsible party than is the case with the GDPR. This may be attributed to some degree to the fact that the GDPR governs EU members where information security, particularly relating to the confidentiality and integrity of data, has been a feature of the social and economic landscapes of those countries for several years. It is also true that in many of these countries government efforts relating to cybersecurity and law enforcement relating to cybercrime are far more advanced than what is the case in South Africa.

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

4.71 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.

4.72 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 must 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 20 and 21]

Notification of security compromises

4.73 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 22]

4.74 The duty to notify a security breach which compromises personal information is relatively novel. First adopted in California and now adopted in all 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.

4.75 The GDPR makes provision in Article 33 for the notification of a personal data breach to the supervisory authority. It expressly provides that the notification shall be without undue delay and, where feasible, not later than 72 hours after having become aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

4.76 The GDPR in Article 34 requires notice of the breach to a data subject only where it is likely to result in a high risk to the rights and freedoms of natural persons. In this instance therefore the Notification of security compromises provision in Section 22 of PoPIA is more onerous on the responsible party with regard to notifying a data subject than the GDPR.

Condition 8

Data subject participation

Access to personal information

4.77 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.

4.78 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 23]

4.79 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 the Act.

4.80 The GDPR provides in Article 15 for a right of access by the data subject which is similar to the corelative provisions in PoPIA.

4.81 The GDPR also recognises the right of the data subject to know if information is being transferred to a third country or an international organisation. The issues of trans-border flows of information need to be considered in the South African context but the onus described does not include information processed within South Africa by an international organisation.

Correction of Personal Information

4.82 This provision deals specifically with the right of a data subject to request a correction or deletion of personal data. The provisions of the Act 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.

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

[Section 24]

4.84 The GDPR in Section 3 deals far more extensively with the correction of personal information, the right to rectification and new rights that have evolved in the European Union like the right of erasure (right to be forgotten) and the right of data portability. These are both rights which have been established by the Court of Justice of the European Union and it is submitted would be taken into consideration by the Information Regulator in recommending amendments to PoPIA as well as in considering the constitutional rights of privacy of data subjects within South Africa.

Manner of Access

4.85 The provisions of sections 18 and 53 of PAIA apply to requests made in terms of Section 34 of the Act.

Chapter 5

5. PROCESSING OF SPECIAL PERSONAL INFORMATION

The aim of this Chapter is to assist the reader's understanding of:

- The prohibition against the processing of special personal information;
- The circumstances in which the processing of special personal information is authorised;
- The specific criteria for authorisation of different categories of special personal information; and
- The processing of personal information of children.

Introduction

5.1 It should be noted that the provisions dealt with in this chapter relate to Parts B and C of Chapter 3 of the Act, which deals with Conditions for Lawful Processing of Personal Information. The Conditions in Part A (dealt with in chapter 4 of this Guideline) also apply to the processing of special personal information.

Prohibition on Processing of Special Personal Information

5.2 Special personal information is information that relates to the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject.

5.3 Special personal information also includes criminal behaviour relating to alleged commissions of offences or any proceeding dealing with alleged offences.

5.4 Unless a general authorisation, alternatively a specific authorisation relating to the different types of special personal information applies, a responsible party is prohibited from processing special personal information.

[Section 26]

General Authorisation

5.5 The prohibition on the processing of special personal information does not apply if:

- consent of the data subject has been obtained;
- processing is necessary for the establishment, exercise or defence of a right or obligation in law;
- processing is necessary to enable compliance with an obligation of International Public Law;
- processing is for historical, statistical or research purposes, subject to stipulated safeguards;
- the data subject has deliberately* made the information public; or

- where specific authorisation has been obtained in terms of the Act.

**The emphasis has been added by the author.*
It should be noted that in certain instances exemptions are provided where information is contained in public records. This is not the case with the general authorisation concerning special personal information and the principle applies only in those cases where the data subject has deliberately made information public. The authorisation provision does not apply merely because personal information is part of a public record. In these instances the data subject may not have deliberately made the information public and particularly if the data subject has not been notified of the processing of the personal information for purposes other than the information being retained in a public record it is likely that this processing would be unlawful.

[Section 27]

Specific Authorisation

5.6 The Act provides separate sections for the authorisation of processing of special personal information. These differ and regard should be had to the specific section governing the authorisation required for processing special personal information.

[Sections 28 to 33]

5.7 The GDPR also includes specific mention of "genetic data" and defines it as personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or health of the natural person. It may be argued that the definition in PoPIA also covers this but it is suggested that in the future the Information Regulator will seek to have PoPIA amended to incorporate specific mention of genetic data.

Processing of Personal Information of Children

5.8 The protection of personal information of children is an issue which is taxing law makers and regulators globally. In certain jurisdictions specific law has been drafted governing the processing of personal information of children. For instance in the United States of America the Children's' Online Privacy Protection Act ("COPPA") protects the personal information of individuals under the age of 13 by mandating compliance with certain conditions that have to be fulfilled before the processing of that personal information can be effected.

5.9 The protection of children under the age of 13 has, following the provisions of COPPA, found favour in many jurisdictions but debates rage as to whether the threshold is too low. In certain jurisdictions distinctions between the process of a child's information (under 13) and a young adult's information (between the ages of 13 and 18) are engaging attention of child right activists and law makers.

5.10 It should be noted that the Act has adopted the United Nations definition of a "child", being a natural person under the age of 18 years, who is not legally competent.

5.11 In essence there is a general prohibition against the processing of personal information concerning a child subject to appropriate authorisation.

5.12 Attention is drawn to the use of the term "competent person". Competent person is defined as "any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child. Importantly a parent or legal guardian may not always be a competent person, although in the vast majority of instances a parent or legal guardian will be a competent person, whose consent must be obtained. There are exceptions in our law where the

consent of a parent or guardian might be replaced by the consent of another party. By way of example a female, regardless of age, may request an abortion, and the consent of a parent or legal guardian is not required. In this instance the competent party is the medical practitioner.

[Sections 34]

5.13 The GDPR in Article 8 provides the age of a child where consent is required is 16 years but also indicates that member states may in their national law provide for a lower age but that the age for a child may not be lower than 13 years.

5.14 The GDPR in Article 8(2) also requires that a controller (responsible party) must make reasonable efforts to verify whether consent has been given, taking into account available technology.

5.15 The authorisation required for the processing of personal information may come by way of:

- the prior consent of a competent person (being a person legally competent to consent to an action or decision by a child);
- information deliberately made public by the child with the consent of a competent person; or
- in the other circumstances in which general authorisation concerning special information may apply.

5.16 It must be recognised that in certain circumstances legislation will render a child "competent". Likewise, there are instances in our law which allow a child to open a banking account at the age of 16. The processing of a child's personal information for this purpose would be regarded as being authorised by virtue of legislation conferring the right on the child.

5.17 The Regulator may also, conditional upon the establishment of appropriate safeguards for the processing of a child's personal information, authorise such processing.

[Sections 35]

Chapter 6

6. **SUPERVISION – INFORMATION REGULATOR**

The aim of this Chapter is to assist the reader's understanding of:

- The establishment of the Information Regulator;
- The legal nature and status of the Information Regulator;
- The powers, duties and functions of the Regulator; and
- The Regulator's powers to exempt the processing of personal information from conditions governing the processing of personal information.

Introduction

6.1 The countries which have succeeded best in introducing protection of personal information legislation (also known as "Data Control", "Privacy" and "Consumer Privacy" legislation) are the countries which have appointed Information Regulators (or Information Commissioners, as they are also known).

6.2 This has been recognised in the GDPR and in Chapter VI "Independent Supervisory Authorities" are dealt with. The requirements are that each member state provides for one or more independent public authorities responsible for monitoring the application of the GDPR. Where more than one supervisory authority has been established in the member state, the member state shall designate a particular supervisory body to represent the member state.

6.3 It must immediately be recognised that the Regulator acts independently of government or a political party, is accountable to the National Assembly and is required to be impartial and perform its functions and exercise its powers without fear, favour or prejudice. The importance of independence of the supervisory body as stipulated in the GDPR is reflected in the requirements for independence of the Information Regulator.

6.4 Article 52(1) of the GDPR expressly provides "Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation".

6.5 The independent status of the Regulator is similar to and should be seen in the light of "State Institutions Supporting Constitutional Democracy" established in terms of Chapter 9 of the Constitution.

6.6 It must also be recognised that the monitoring and enforcement of compliance by the Regulator is only one of the many facets of its overall responsibility. The protection of personal information is a novel jurisprudence in South Africa and because of the pervasiveness of information and the continuously and very rapidly changing landscape relating to the processing of personal information, the regulation of the protection of personal information will require a flexible approach. However, it is also important that legal certainty is established wherever possible. The Regulator should assist in providing the flexibility required and establishing the legal certainty that we desire.

6.7 In comparing the role of the Regulator in providing a body of law governing the protection of personal information, the Regulator's powers may be seen in similar light to those of the Commissioner of Inland Revenue. Our tax laws and their implementation are in a constant state of flux and often have to be interpreted to provide practicality and certainty. The Commissioner of Inland Revenue is empowered and provides rulings which create a framework of relative certainty, critical to our economic well-being. Hopefully, the Regulator will, as technologies and applications of technologies develop, also be able to act against abuses and provide guidance as to the appropriate processing of personal information.

6.8 The Regulator will need to address novel issues with due regard to legal principles, and where possible, evaluate the functional equivalence that established legal principles would bear to these novel circumstances.

Structure

6.9 The Regulator consists of a chairperson and four other persons as ordinary members of the Regulator. The members of the Regulator will need to be fit and proper persons and have appropriate qualification, expertise and experience to fulfil their role. Currently the chairperson is appointed in a fulltime capacity, as well at two of the ordinary members. The other two have been appointed in a part-time capacity.

6.10 The Act provides for the appointment of a chief executive officer, management and staff appropriate for the work to be performed by the Regulator.

[Sections 41]

6.11 The Act also provides for the establishment of an Enforcement Committee, comprising at least one member of the Regulator and other members appointed by the Regulator. The Enforcement Committee will be chaired by an active or retired judge of the High Court of South Africa, or a magistrate, advocate or attorney with at least 10 years' appropriate experience.

[Sections 50]

Powers, Duties and Functions of the Regulator

6.12 The Regulator's powers, duties and functions are to:

- provide education, including the promotion of understanding and acceptance of the Conditions of Lawful Processing of Personal Information;
- monitor and enforce compliance through the powers vested in it by the legislation;
- consult with interested parties on a national and international basis;
- handle and investigate complaints;
- conduct research and report to Parliament on international developments;
- assist in the establishment and development of codes of conduct;
- facilitate cross-border cooperation in the enforcement of privacy laws with other jurisdictions; and
- generally do everything necessary to fulfil these duties, and foster a culture which protects personal information in South Africa.

[Sections 40]

6.13 The Regulator's powers in terms of the Promotion of Access to Information Act ("PAIA") are dealt with in the Schedule to the Act. The Schedule details amendments to PAIA, and in particular introduces Chapter 1A, which deals with how the Regulator will deal with complaints in terms of PAIA. These changes are dealt with in greater detail in Chapter 15 of this Guideline.

Chapter 7

7. DIRECT MARKETING BY MEANS OF UNSOLICITED ELECTRONIC COMMUNICATION

The aim of this chapter is to assist the reader's understanding of the rights of data subjects regarding:

- Direct marketing by means of unsolicited electronic communications;
- Directories; and
- Automated decision-making.

Introduction

7.1 Direct marketing has existed for a long time. However, the advent of electronic communication and its refinement into social networking platforms has led to enormous abuses of personal information. This includes the use of personal information to perpetuate frauds, often prevalent in electronic banking, credit card transactions and other commercially-related fraudulent activity.

7.2 One of the abuses of personal information is that data subjects are flooded with unsolicited electronic communications (SPAM), which for the most part is entirely unwelcome and provided from sources with which data subjects want no interaction. In many jurisdictions this has led to anti-spam legislation. The issue was not initially within the remit of the SALRC but, due to public demand and the recognition of the magnitude of the problem, the SALRC, and in turn the PPC, have been required to deal with this issue.

7.3 It should be noted that direct marketers in certain circles appear to be basing an argument that they are entitled to continue direct marketing by electronic means without complying with Section 69 of the Act, by virtue of the provisions of Section 11(1)(f), which provides that personal information may only be processed if processing is necessary for pursuing the legitimate interests of the Responsible Party or of a third party to whom information is supplied. While it is beyond the scope of this Guideline to deal with all of the legal issues, this is a weak attempt to negate the clear intention of the legislature to prohibit direct marketing by electronic means, unless it meets the criteria established in Section 69.

Direct Marketing by Means of Unsolicited Electronic Communications

7.4 The general principle reflected in Section 69 is that if the data subject does not consent to the processing of his, her or its personal information for the purposes of direct marketing, the Responsible Party will not be allowed to use the data subject's personal information for this purpose. The Responsible Party is allowed to approach a data subject (by whatever means) in order to request the consent of the data subject. The Responsible Party cannot approach the data subject for consent on more than one occasion.

7.5 The data subject must be given a reasonable opportunity to object to the processing of his, her or its personal information when the information is collected, and on any occasion that the

information is used for the purpose of marketing if the data subject has not already refused to allow use of the information for this purpose.

7.6 Should the data subject object, any further processing of the information for this purpose is a breach of the provisions of Section 69.

[Sections 69]

7.7 Attention is drawn to the proposal concerning the respect for private life and the Protection of Personal Information in electronic communications that has been tabled before the European Parliament ("The EU ePrivacy Regulation"). The proposal in its current form has been approved by the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee). It contains strict provisions relating to the use of numerous forms of electronic communication, the processes of direct marketing and profiling. This will have a far-reaching effect on direct marketing and as has previously been stated it is likely that the Information Regulator will follow the European example in this regard.

7.8 The GDPR in Article 21 also provides that where personal data are processed for direct marketing purposes or profiling the data subject has a right to object.

7.9 Profiling is defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;".

Directories

7.10 The data subject must be informed, free of charge, before the data subject's personal information is included in a directory, about the purpose of the directory and any further uses to which the directory may possibly be put.

7.11 A data subject must be given a reasonable opportunity to object free of charge, and obtain confirmation that the Responsible Party has withdrawal the data subject's personal information from the directory.

[Sections 70]

Automated Decision-Making

7.12 In many instances people have become subject to decisions which are made by computers. As a result there are cases where the results of the decision may be influenced by incorrect data, incomplete data or simply by circumstances which are not taken into account in programming the basis on which the computer may make an automated decision. In the circumstances the provisions relating to automated decision-making confer on the data subject the right to be provided with an opportunity to make representations about a decision and require information pertaining to the underlying logic on which the processing of the information occurred, to enable the data subject to make representations to the Responsible Party.

[Sections 71]

Chapter 8

8. **TRANS-BORDER INFORMATION FLOWS**

The aim of this Chapter is to assist the reader's understanding of:

- Why trans-border flows need to be regulated;
- Practical issues of trans-border flows of information; and
- Compliance with the provisions of Chapter 9.

Adequacy and Safe Harbour Agreements

8.1 Information knows no borders and in an effort to protect the personal information of data subjects within the European Union, the European Union's 1995 Privacy Directive provides that member states should prohibit the transfer of personal information to countries that do not have adequate law to protect the information. This has motivated many countries (including South Africa) to enact laws that meet the adequacy requirements of the European Union, particularly where they are trading partners of European Union countries.

8.2 The GDPR devotes Chapter V to transfers of personal data to third countries or international organisations. Article 44 sets out the general principle for transfers of personal information across borders. As this is more the definitive summary for trans-border flows of information, Article 44 is quoted in full:

> *"44. Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."*

8.3 It is important to note that the adequacy requirement in the GDPR no longer refers purely to "adequate law". In determining adequacy account must be taken of:

8.3.1 The rule of law effect for fundamental rights and freedoms and relevant legislation protecting the privacy of personal information;

8.3.2 The existence and effective functioning of an independent supervisory authority (Information Regulator); and

8.3.3 International commitments the third countries or international organisation has concluded relating to the protection of personal data.

8.4 One of the non-negotiable components of adequacy is that the laws of that country, in turn, prohibit trans-border flows of information, subject to appropriate safeguards. The purpose of this protection is obvious as it would not serve to protect information from European Union countries if processors of information in that country could transfer the information to another country which does not offer adequate protection.

8.5 Prior to these provisions that will become effective on the 25th May 2018, under the European 1995 Privacy Directive to enable European Union countries to exchange personal information with the USA, which did not have "adequate law", the Safe Harbour Accord was agreed governing the transfer of personal information from EU member countries and the USA. As a result of revelations by Edwin Snowden indicating that the personal information of European Union citizens had been accessed by the National Security Agency in the USA, Max Schrems, at the time a 28 year old law student, referred this issue to the European Union Court of Justice. The court struck down the existing Safe Harbour Accord and it became necessary to renegotiate the basis on which the personal information of European Union citizens could be processed in the USA. This has led to the development of what is known as the "Privacy Shield", an agreement that now governs transfers of European Union citizens' personal information and its processing in the USA.

8.6 While there were several motivations for the revision of the Data Protection Act in the United Kingdom, one of the primary motivations was the United Kingdom's exit from the European Union. This has led to a review and revision of the existing Data Protection Act in England, among the amendments being revisions that ensure that the United Kingdom would be considered to have adequate law and can receive and access information from European Union member countries.

Development of Privacy Law

8.7 The global importance of privacy law and the protection of personal information is highlighted by the development of legislation in many countries across the globe to deal with this issue and provide adequate protection for the processing of personal information.

8.8 Today in excess of 80 countries around the world have enacted privacy legislation and there are many more which are in the process of developing and enacting privacy legislation. In Africa, the African Union in June of 2014 adopted the African Union Convention for Cybersecurity and Personal Data Protection which has been signed by 8 of the European Union countries but not yet by South Africa.

8.9 As already indicated in this Guideline, the USA, having up to now protected the privacy of consumer information at a State level, has through the period of the Obama Administration seen growing pressure for federal legislation to be enacted addressing consumer privacy. While the Trump Administration has professed a different view on the privacy of personal information, there are strong lobbies that continue to pressurise the Trump Administration in this regard. These lobbies, allied to the strong stance taken by the European Union and other democracies globally on the issue of privacy, seem to have prevented changes to privacy law that were made in campaign promises by President Trump.

8.10 In South Africa the ruling party and in particular the Department of Justice has been remiss in delaying the implementation of the PoPIA, enacted as long ago as 2013. This delay, allied to the fact that Parliament has failed to provide adequate budget and resource to the Information Regulator to enable the Information Regulator to effectively and efficiency carry out the duties that PoPIA imposes, is regrettable.

8.11 This having been said there are promising signs that the Information Regulator is guarding its independence and working hard to meet the strategic objectives that it has set itself. This will be extremely important in promoting the adequacy and the level of protection of personal information of data subjects that is demanded by the GDPR. In this regard it is important to note that the EU will, on an ongoing basis, monitor developments in third countries and international organisations and give guidance to its members on transfers of personal information to third countries and international organisations.

Transfers of Personal Information outside the Republic

8.12 A Responsible Party in the Republic may not transfer personal information about a data subject to a third party which is in a foreign country unless adequate levels of protection are provided by:

- the law of the country;
- binding corporate rules of the Operator to which information is provided;
- a binding agreement between the Responsible Party in the Republic and the Operator in the foreign country;
- the law, corporate rules or binding agreement must effectively uphold the principles of reasonable processing, similar to the Conditions of Lawful Processing in Chapter 3 of the Act.

8.13 There are other justifications for the transfer of trans-border information flows which include the consent of the data subject. These should be considered in any event in determining how the information is to be processed, if it is to be processed in a foreign country. The development of cloud computing, which in many cases will allow for the processing of information outside of the borders of the Republic, is subject to this provision. Any agreements which relate to cloud computing need to be carefully examined to ensure that the provisions governing trans-border information flows are not contravened.

[Sections 72]

Chapter 9

9. THE ROLE OF THE INFORMATION OFFICER IN MODERN BUSINESS

The aim of this Chapter is to assist the reader's understanding of:

- The role of the Information Officer within an organisation;
- The duties and responsibilities of an Information Officer in terms of both PoPIA and PAIA; and
- Considerations for the appointment of an Information Officer.

Information Officer

9.1 As the information age progresses, the necessity of developing the functions of governing, managing and securing information has become ever more important. Designations within organisations of "Information Security Officer" and "Information Officer" have become increasingly prevalent. It is important to recognise that these are not information technology functions. They relate to a business's information as opposed to the mechanisms used to process the information. While the information technology function has a very important role in ensuring that appropriate technologies are used and are configured to provide adequate safeguards to the information processed, it is a business responsibility to ensure that the information is properly managed and protected according to classifications and security safeguards determined by business.

9.2 Increasingly we are seeing legislation require that the responsibility for an organisation's information is specifically designated. PAIA and the Act both expressly provide for the appointment of an information officer (in the case of PAIA the head of a private body is assigned this role and if the private body is a juristic person, the chief executive officer may designate the role to a duly authorised officer of the juristic person)[10]. There are several other legislative instruments that also define issues relating to the management and security of information without necessarily designating an information officer. Also, in terms of Generally Accepted Information Security Practice, the appointment of an information officer for the purpose of monitoring the establishment and maintenance of information security on a day to day basis is recommended. This will in certain circumstances be a responsibility to be discharged by a person as part of other responsibilities, while in other circumstances it may be a fulltime role.

9.3 The predominance of law firms within South Africa are relatively small. In these circumstances the role of the Information Officer will probably be exercised by a partner and would form part of the administrative functions often performed by partners in the conduct of the business of their practice. In terms of both PAIA and PoPIA the Information Officer would be:

- In the case of a sole practitioner, the sole practitioner or any person duly authorised by the sole practitioner;

[10] Definition of "Head" in Section 1 of PAIA

- In the case of a partnership, any partner of the partnership or any person duly authorised by the partnership;
- In the case of an incorporated practice, the chief executive officer or a person duly authorised by the chief executive officer;
- In the case of a public body, for instance, the new Legal Practices Council, the chief executive officer or the person acting as such.

Designation and Delegation

9.4 Provision is made in PAIA for the appointment of deputy information officers as well and this is followed in PoPIA.

Duties

9.5 Private bodies (which includes all attorneys' firms) must designate the responsibilities of an Information Officer (or deputy information officers where appropriate) to perform the duties required in the Act. Similarly, the duties to deal with requests for access to information in the case of private bodies must be discharged by the Information Officer (failing the delegation of these duties to a specific Information Officer, these duties have to be discharged by the person who is required to do so in terms of PAIA and PoPIA.

[Sections 1 (Definition of "Head") and 17 of PAIA]

9.6 the Act provides that an Information Officer's responsibilities include:

- encouragement of compliance with the Conditions for the Lawful Processing of Personal Information;
- dealing with requests pursuant to this Act;
- interaction with the Regulator; and
- otherwise ensuring compliance with the provisions of the Act.

[Sections 55 and 56]

9.7 Attention is also drawn to Regulation 4 in the draft Regulations published by the Information Regulator which sets out the duties of Information Officers. It should be noted that the draft Regulations are subject to comment and changes may be made to this Regulation. It is likely, however, that the duties of information officers will remain materially similar to those stipulated in the draft Regulations.

9.8 There are numerous areas that require action by duly appointed information officers and PAIA should be read with specific reference to the rights and obligations of parties in terms of PAIA in determining the duties of the Information Officer.

9.9 However, one of the primary functions of the Information Officer is the receipt, processing and determining whether access to information held by the private body should be granted.

9.10 The mechanisms for requests for access to information should be established in a manual where the private body has established a manual. Where this is not the case it is suggested that information officers familiarise themselves with the provisions of Sections 51 to 61 of PAIA to

ensure that requests for access to information are properly processed and that the necessary documentation for this purpose is established.

9.11 Assuming that a request for access to information has been properly made, the person adjudicating the request (it is suggested that this is the Information Officer who should be assisted by persons within the organisation who provide information relating to whether the request should be granted) be fully aware of the provisions of Chapter 4 of PAIA dealing with the grounds for refusal of access to records. It should also be noted in the context of PoPIA that there are mandatory protections of the privacy, commercial information, confidential information, information relating to the safety of individuals and protection of property. Of specific import to attorneys is the mandatory protection of "privileged" information.

9.12 It must also be borne in mind that both in the case of public and private bodies there is an obligation to assist the requestor in the proper processing of the request. This will include, without limitation, assistance in the completion of any forms, the acknowledgement of receipt of the request, the clarification of requests and where necessary, the transfer of requests to an appropriate public body which may be in possession of the records requested.

Qualifications for Information Officer

9.13 No formal qualifications are required for an Information Officer but anybody who holds this position by way of legislation or who is delegated the responsibilities of an Information Officer must familiarise themselves with the provisions of PAIA and PoPIA if they are to fulfil their duties properly. It is also recommended that in view of the importance of security of personal information and the fact that the grant of access to information to a third party is in itself an element of information security, that an Information Officer must become aware of the information security that is appropriate in respect of the information processed by the firm. This is not a function that can be delegated or outsourced to a third party, although the assistance of third parties may be useful. It should be a core competency of any modern organisation. It is far better that the person delegated to this position is familiar with and understands the value of information processed by the organisation and what information security would be appropriate with regard to the information, than to appoint a person who is unfamiliar or does not appreciate the value of the information within a particular organisation. It is also easier to learn about the disciplines of information security that need to be applied within an organisation than to provide an Information Officer with the necessary background and experience of a firm or its workings within a profession.

9.14 It is suggested that with larger organisations persons who are appointed as Information Officers should be provided with proper training in information security (this is not purely technological) and their obligations in terms of various elements of legislation in South Africa.

Chapter 10

10. **PRIOR AUTHORISATION**

The aim of this Chapter is to assist the reader's understanding of:

- When prior authorisation for the processing of personal information is necessary; and
- Notification to the Regulator.

Processing Subject to Prior Authorisation

10.1 Prior authorisation is necessary where the Responsible Party plans to process information:

- which contains any unique identifiers of data subjects for a purpose other than the one specifically intended at collection and with the aim of linking the information being processed with information processed by Responsible Parties;
- in respect of criminal, unlawful or objectionable conduct;
- for the purpose of credit reporting;
- that is defined as special personal information or is the information of a child which is being transferred to a foreign country that does not provide an adequate level of protection in its law.

10.2 The Regulator may require prior authorisation if the processing carries a risk to the legitimate interests of the data subject.

10.3 Prior authorisation is not necessary where a code of conduct governing the processing of the personal information has been issued and come into force.

10.4 The authorisation only has to be obtained once for a particular category of processing but if the manner of processing changes then a further application to the Regulator for authorisation will be necessary.

[Section 57]

10.5 Attention is drawn to the fact that the draft Regulations published by the Information Regulator do not address the issue of prior authorisation. This is a surprising omission and comment has been addressed to the Regulator in this regard.

10.6 In the absence of express direction from the Information Regulator, responsible parties would do well to consider the provisions of Section 3 (Articles 35 and 36) of the GDPR that deal with "data protection impact assessments" and "prior consultation."

10.7 It is strongly recommended that any project addressing Protection of Personal Information and compliance with the conditions for lawful processing of personal information includes the conduct of privacy impact assessments and consultation with the Information Regulator to ensure that

measures taken by the responsible party are adequate for the protection of personal information processed by it.

Notification to Regulator

10.8 the Act provides for the circumstances and manner in which notification must be made to the Regulator, time periods applicable and consequences of non-compliant processing.

10.9 The failure to notify processing subject to prior authorisation is an offence.

[Sections 58 and 59]

Chapter 11

11. **CODES OF CONDUCT**

The aim of this Chapter is to assist the reader's understanding of:

- The purpose of codes of conduct; and
- The Regulator's obligations and responsibilities in this regard.

Introduction

11.1 The processing of information is diverse and extends across many different sectors of our commercial world. There may be varying considerations governing the processing of personal information in different sectors which require sharper definition than is possible in framework legislation of the nature of the Act. For this reason provision is made for the establishment of codes of conduct which will govern the processing of personal information within defined sectors.

11.2 The codes of conduct will not mean that a particular sector may enjoy a more relaxed regime relating to the processing of personal information. The Act expressly provides that a code must incorporate all of the Conditions for the Lawful Processing of Personal Information or obligations that are a functional equivalent of those conditions. The intention is merely to give Responsible Parties operating in specific sectors governed by codes of conduct, clearer guidance on how they may process personal information.

The Regulator's Obligation

11.3 The Regulator may of its own accord but in consultation with stakeholders issue a code of conduct. Alternatively, the far more likely scenario is that the Regulator will, on the application of a body representative of an industry, profession, or vocation assist in the development and issue of a code of conduct.

[Section 60]

11.4 Codes of conduct may prescribe procedures for dealing with complaints, provided that they do not restrict the Regulator's powers of enforcement provided for in the Act.

11.5 As long as they meet the requirements of the Regulator, codes may set out procedures dealing with and governing the addressing of complaints to an adjudicator appointed by the particular industry, profession or vocation. A Responsible Party aggrieved by the determination by an adjudicator may submit the complaint to the Regulator but the adjudicator's determination continues to have effect unless and until the Regulator determines otherwise.

11.6 The Regulator has the power to revoke codes of conduct.

11.7 The Regulator may develop and provide written guidelines relating to the establishment of codes of conduct and must work with members of the relevant sector in doing so. The Regulator may review the operation of an approved code of conduct.

11.8 A code of conduct will become effective after the prescribed period of notification in the Government Gazette and bind the applicable industry, profession or vocation.

[Section 62]

11.9 Failure to comply with the code of conduct is deemed to be a breach of the Conditions of Lawful Processing of Personal Information and is subject to the enforcement provisions of the Act.

11.10 The GDPR, in Section 5 (Article 40 to 43) deals with codes of conduct and certification. PoPIA does not deal with certification and while the provisions of the GDPR may be helpful, it is suggested that they will have little impact on codes of conduct under PoPIA, save to the extent that the Information Regulator may develop regulations governing codes of conduct that are aligned to the provisions of the GDPR.

Chapter 12

12. **ENFORCEMENT**

The aim of this Chapter is to assist the reader's understanding of:

- The approach to enforcement of a data subject's rights;
- The steps to be followed in dealing with a complaint made to the Regulator; and
- The Regulator's rights of enforcement.

Introduction

12.1 Chapter 10 of the Act, dealing with "Enforcement", reflects the intention of creating both a "light touch" enforcement where essentially the Regulator is required to mediate complaints relating to wrongful or unlawful processing of personal information, allied to the Regulator's powers to investigate complaints, assist data subjects in the enforcement of their rights, and where necessary, impose administrative fines.

12.2 This approach is based on approaches taken in jurisdictions that have appointed Information Commissioners or Regulators. As these regulators have matured in other jurisdictions, they have called for and in many cases received additional powers and the authority to impose heavier sanctions.

12.3 This is illustrated by the GDPR that stipulates administrative fines of up to €20 000 000.00 (Twenty million Euros) [approximately R300 000 000.00 (Three hundred million Rand) at the time of writing] or 4% of the global worldwide annual turnover for the preceding financial year, **whichever is higher,** may be imposed for breaches of the GDPR. The maximum administrable fine under PoPIA is R10 000 000.00 (Ten million Rand). This discrepancy can be attributed partly to time (the wording of PoPIA was finalised in 2011) and the increasing seriousness that the democratic world is taking to privacy breaches. It is also submitted that the flexibility created by linking the penalty to turnover, is an amendment that the Information Regulator may well propose to Parliament.

12.4 It is also hoped that the provisions assist data subjects in enforcing their rights in terms of both PAIA and PoPIA, which often simply do not warrant delays and the expense of going to court. The common experience of denial of access to information in terms of PAIA, which are in many instances transparently wrongful and unjustified, motivated the provision of powers to the Regulator to enforce, in particular, the Conditions Governing the Lawful Processing of Personal Information and a data subjects right of access to information in terms of PAIA.

12.5 This Guideline is intended to provide information as to the provisions in the Act but attorneys are urged to gain a full understanding of the operation of the enforcement provisions in Chapter 10 and to monitor the requirements of the Regulator relating to enforcement. The provisions of the PoPIA will no doubt be supplemented by Regulation and practice directives issue by the Information Regulator in the future. These provisions, read with a clear understanding of the Conditions for the Lawful Processing of Personal Information contained in Chapter 3, are critical to an attorney providing advice to and assisting clients in the protection or prosecution of their rights.

Interference with the Protection of Personal Information of Data Subject

12.6 Chapter 10 of PoPIA commences with defining what constitutes interference with the protection of personal information which includes a breach of any of the conditions for the lawful processing of personal information, non-compliance with various sections of the Act, including among others, failure to notify a security compromise, direct marketing by electronic communication in contravention of the provisions governing direct marketing, and transfers of personal information outside of the Republic in breach of the provisions governing those transfers. It also includes breaches of codes of conduct which may be established for a particular industry or professional vocation.

[Section 73]

12.7 The manner of submitting a complaint, the actions of the Regulator on receipt of the complaint, and the Regulator's decision as to what action is appropriate are established. After considering and investigating the complaint (where it is felt necessary), the Regulator must advise a data subject submitting the complaint as to the action that it may or may not take regarding the complaint. The Regulator may also, if it considers another regulatory body more competent or appropriate to deal with the complaint, to refer the complaint to that body.

[Sections 74 to 78]

Pre-investigation and Settlement of Complaint

12.8 Before proceeding with an investigation, the Regulator must notify the data subjects to whom the complaint may relate and the Responsible Party of the details of the complaint and the subject matter of the investigation. The Responsible Party must also provide a reasonable period in which to respond in writing to the complaint.

12.9 Where the Regulator deems it may be possible to secure a settlement or satisfactory assurances against repetitions of offending actions, the Regulator may attempt to secure such settlement or assurance.

[Sections 79 and 80]

Investigation by Regulator

12.10 PoPIA stipulates the powers enjoyed by the Regulator which will enable proper investigation of complaints to the Regulator and include the summoning and appearance of persons before the Regulator to provide oral evidence on the issue and execution of warrants, matters exempt from search and seizure (including communications between legal advisors and clients) and how objections to search and seizure may be dealt with.

[Sections 81 to 88]

Assessments

12.11 The Regulator may, on its own initiative or on behalf of a Responsible Party, data subject or any other person, assess whether the processing of personal information complies with the provisions of the Act.

12.12 The Regulator is obliged to make assessments where it appears appropriate, unless the Regulator is unable to satisfy itself as to the identity of the person making the request or to identify the action in question. Section 77 deals with matters which the Regulator must take into account in assessing the appropriateness of the assessment and where the assessment is made on request, notify the requestor of the actions taken.

[Section 89]

Information Notice

12.13 The Regulator may either on request, alternatively if the Regulator reasonably requires, serve on a Responsible Party an information notice requiring the Responsible Party to furnish to the Regulator, within a specified period, a report indicating that the processing is taking place in compliance with the provisions of the Act or such information relating to the request for compliance with the Act as may be specified in the notice.

12.14 The form of the notice and what information may be requested is specified and is likely to be further amplified by regulations and prescribed forms which may be developed by the Regulator, once appointed.

Parties to be Informed of Result of Assessment

12.15 After completion of an assessment the Regulator must inform interested parties and may, where appropriate, require a Responsible Party to implement the recommendations contained in the report. The report may, if the Regulator considers it to be in the public interest, be made public and may be deemed to be an enforcement notice (more fully dealt with later in this chapter).

[Section 91]

Enforcement Committee

12.16 PoPIA provides for the establishment by the Regulator of an enforcement committee. The purpose of the enforcement committee is to consider all matters referred to by the Regulator in terms of the Act and PAIA. After considering submissions made by parties, the enforcement committee must make findings which are to be reported to interested parties and recommendations to the Regulator relating to further action which may be taken.

[Sections 92, 93 and 94]

Enforcement Notice

12.17 If the Regulator is satisfied (after considering the recommendations of the enforcement committee) that a Responsible Party is interfering with the protection of personal information it may serve an enforcement notice on the Responsible Party.

12.18 The enforcement notice may require the Responsible Party to take specified steps or desist from actions specified by the Regular within the period stipulated in a notice. Enforcement notices will have to be in the form provided for in the Act or as may be determined by the Regulator from time to time.

[Sections 95 and 96]

12.19 PoPIA makes provision for appeals against enforcement notices, which may be made to the High Court having jurisdiction, for the variation or setting aside of the enforcement notice.

[Section 98]

Civil Remedies

12.20 PoPIA provides that a data subject or a Regulator on the request of the data subject may institute civil action against a Responsible Party arising from an interference with protection of personal information, whether or not there is intent or negligence on the part of the Responsible Party. Defences that may be raised by a Responsible Party are specified. The manner in which the Regulator required to deal with the distribution of awards or damages granted where the Regulator institutes civil actions for damages on behalf of a data subject is also dealt with.

12.21 It is also interesting to note that where civil actions have not been instituted agreements of settlement may be made orders of court and must be published in the Gazette and such other public media announcements as the court considers appropriate may need to be made. This allows not only for the public becoming aware of its rights, but also poses potential reputational risk issues for Responsible Parties who do not comply with the provisions of the Act.

[Section 99]

Chapter 13

13. **OFFENCES, PENALTIES AND ADMINISTRATIVE FINES**

The aim of this Chapter is to assist the reader's understanding of:

- What penalties may be imposed for offences; and
- The issue of administrative fines.

Introduction

13.1 The Chapter, among others, creates offences such as obstruction of the Regulator, breach of confidentiality by a person acting under the direction of the Regulator, failure to comply with an enforcement notice, unlawful acts by Responsible Parties in connection with account numbers of data subjects and unlawful acts by third parties in connection with account numbers of data subjects.

13.2 More serious offences, which include the hindering, obstruction or unlawfully influencing the Regulator, failure to comply with an Enforcement Notice, giving false evidence, contravening the Lawful Conditions for the Processing of Personal Information in so far as they relate to an account number (being a unique identifier assigned to one data subject or jointly to more than one data subject by financial institutions) are punishable by a fine (no limit to the fine is stipulated) or to a period of imprisonment not exceeding 10 years, or both a fine and imprisonment.

13.3 Less serious offences (of a more technical or procedural nature) may be punishable by a fine (no limit on the fine is stipulated) or imprisonment for a period of 12 months, or both a fine and such imprisonment may be imposed.

13.4 A magistrate's court has the jurisdiction to impose the penalties contemplated above.

[Sections 100 to 108]

Administrative Fines

13.5 The Regulator may deliver infringement notices on Responsible Parties who have failed to comply with the Act, specifying, among other issues, the particulars of the alleged offence and the amount of the administrative fine payable. The limit of administrative fines which may be imposed by the Regular is R10 000 000.00 (Ten million Rand). Should the infringer not comply with the notice, the Regulator may file with the clerk or registrar of a competent court, a statement setting forth the amount of the fine and the statement will thereupon have the effect of a civil judgement lawfully granted in a court in favour of the Regulator for a liquid debt in the amount specified in the statement.

13.6 Where administrative fines are imposed no prosecution is instituted against the Responsible Party and the administrative fine does not constitute a previous conviction in terms of the Criminal Procedure Act.

[Section 109]

13.7 The GDPR shows a trend to imposing more serious penalties on contraventions of the GDPR. It allows that administrative fines of up to €20 000 000.00 (Twenty million Euros) [approximately R300 000 000.00 (Three hundred million Rand) at the time of writing] may be imposed, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year of the undertaking, **whichever is the higher**.

13.8 It is quite possible that in view of the low penalties that are imposed in PoPIA that it may be necessary for the Information Regulator to recommend to Parliament that the penalties contained in PAIA, already at least 7 years out of date, are significantly increased.

Chapter 14

14. **GENERAL PROVISIONS**

The aim of this Chapter is to assist the reader's understanding of:

- The transitional arrangements for the introduction of the Act.

Introduction

14.1 As is usual with most legislation the general provisions allow for the amendment of legislation, fees which may be prescribed by the Minister or Regulator, establishment of regulations and the procedure for making regulations.

[Sections 110 to 113]

Transitional Arrangements

14.2 the Act provides that all processing of personal information must conform to the provisions within 1 year after commencement of the Act. Thus, until the expiry of that year, any Responsible Party processing personal information, **even where the processing commenced before the enactment of the Act**, does not fall foul of the provisions governing the lawful processing of personal information during that year (or such extended period as the Minister may determine).

14.3 Immediately after the expiry of the transitional period (one year or such extended period as the Minister may determine) all processing of personal information of whatever nature will be subject to the provisions of the Act.

14.4 The requirement of prior authorisation contemplated in Sections 57 and 58(2) will not apply until the Regulator determines otherwise by notice in the Gazette.

14.5 The South African Human Rights Commission is also required to attend to the conclusion of its functions and the transfer of this responsibility to the Regulator in terms of PAIA as soon as reasonably possible after the amendment of those sections in PAIA required in the Schedule to the Act.

[Section 114]

Chapter 15

15. THE PROMOTION OF ACCESS TO INFORMATION ACT 2000

The aim of this Chapter is to assist the reader's understanding of:

- The transfer of the obligations of the South African Human Rights Commission to the Regulator; and
- Future regulation in enforcement of PAIA by the Regulator.

Introduction

15.1 It is widely recognised that the South African Human Rights Commission has not fully succeeded in its role as the regulator of PAIA. Many requests for access to information are improperly and obstructively dealt with by persons who have information in their possession or under their control.

15.2 The perpetrators of this negation of the constitutional right to access of information rely on the fact that the sole remedy of the requestor in combatting the perpetrators malfeasance is to make an application to court, which in many instances is not warranted due to the delays and costs involved in this process.

15.3 Against this background and the difficulty in obtaining access to information due to this unconscionable behaviour, the recommendations of the SALRC, that the Regulator be given powers to regulate both the Act and PAIA have been accepted by the legislature. This is in alignment with many international jurisdictions where the Regulator has the powers to regulate both privacy and access to information rights.

Amendments to PAIA

15.4 To a large extent the amendments to PAIA (set out in the Schedule to the Act) are aimed at harmonising the provisions of the Act and PAIA and affecting consequential changes where it is necessary to do so.

15.5 The most significant amendment is the fact that breaches of PAIA will be dealt with by the Regulator in terms of enforcement provisions substantially similar to those stipulated in the Act.

15.6 It is hoped that the powers of enforcement granted to the Regulator will prevent the abuses by parties having information under their control (not exclusively personal information) who obstruct legitimate access to the information.

15.7 The reader's attention is drawn to the amendments reflected in Chapter 1A of PAIA and numbered 77A through to 77K.

15.8 The amendment of Section 78 of PAIA in line with the ruling of our Constitutional Court, extending the period for appeals from 30 days to 180 days is effected in 19 of Schedule 2 to PoPIA.

[Schedule 2 of the Act]

Chapter 16

16. **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

16.1 This report documents the research conducted principally by Advocate Ananda Louw the Principal State Law Advisor, and provides 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.

16.2 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

Michalsons Attorneys

16.3 Michalsons Attorneys' website **https://www.michalsons.com/** offers assistance in addressing many of the vastly differing issues that are faced by organisations initiating both the protection of personal information and General Data Protection Regulations projects. The Michalsons' website is dynamic, well maintained and updated regularly with new issues that may be facing practitioners and clients in their privacy initiatives.

16.4 Michalsons have also contributed to the Global Privacy Security Law publication addressing privacy law and PoPIA. This chapter and references to the book can be accessed at **https://www.michalsons.com/blog/global-privacy-data-protection-book/4794**.

"A Guide to the Protection of Personal Information Act" authored by Elizabeth de Stadler and Paul Esselaar

16.5 The book is valuable in establishing a basic guideline in addressing PoPIA and providing examples that may be helpful to persons wishing to understand the Act.

"Information and Telecommunications Law" published by Lexis Nexis.

16.6 Chapter 8 of this publication deals with data protection. The author of this Chapter, Professor Anneliese Roos, provides a commentary on PoPIA as initially proposed by the SALRC which is useful. However, care needs to be taken in considering this commentary as significant amendments have been made to the initial version of PoPIA since the commentary was drafted.

Information Commissioners, Supervisory Authorities or Regulators

16.7 The offices responsible for the governance of data protection in different countries has been assigned different names. Typically in Europe they are called "commissioners" or "data protection authorities". Canada, Australia and New Zealand all refer to "information commissioners" or "privacy commissioners". Typically these commissioners have addressed data privacy issues which will be of relevance to South Africa and made rulings in this regard. The guidelines and rulings of the commissioners will prove to be very valuable in considering the treatment of the Protection of Personal Information in South Africa and it is recommended that they be consulted.

16.8 As it is highly likely that the Information Regulator will be guided by decisions of the European Data Protection Supervisor (EDPS) (which oversees all data protection authorities in the European Union) it is suggested that the guidance provided by the EDPS is consulted. The Information Commissioner in the United Kingdom is also a valuable source of information with clear and concise guidelines covering both United Kingdom legislation and guidance to the GDPR and its implications for the United Kingdom.

16.9 The reader is referred to the web addresses of the following commissioners, regulators and supervisory authorities:

- The European Data Protection Supervision **www.edps.europa.eu**
- 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

16.10 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**.

Important Developments in 2012

16.11 The European Parliament and Council have proposed a directive which is being considered by the member states. Along with this they have proposed a regulation (which will govern all of the member states) relating to the protection of individuals with regard to the processing of personal data and on the free movement of such data. This development sees a strengthening of the stance of the European Union relating to the protection of personal data from that initially taken in providing the privacy directive in 1995. These were published by the European Union in early 2012 and can be found at **www.ec.europa.eu/home-affairs/doc_centre/police/docs/com_2012_10_en.pdf**.

16.12 In the United States of America President Barack Obama introduced "Consumer Data Privacy in a Networked World : A Framework for Protecting Privacy and Promoting Innovation in a Global Digital Economy" which seeks the enactment of federal law governing the protection of personal information of America's citizens. This may be found at **www.whitehouse.gov/sites/default/files/privacy-final.pdf**.

16.13 The Federal Trade Commission published "Protecting Consumer Privacy in an Era of Rapid Change – Recommendations for Businesses and Policymakers" which supports the enactment of federal legislation and pledges the Federal Trade Commission's support to the consideration of enacting baseline privacy legislation in the United States of America. This report can be found at **www.ftc.gov/os/2012/03/120326privacyreport.pdf**.

16.14 Daily feeds, which deal with global developments relating to privacy, are accessible through the International Association of Privacy Practitioners' website (**https://www.privacyassociation.org**).