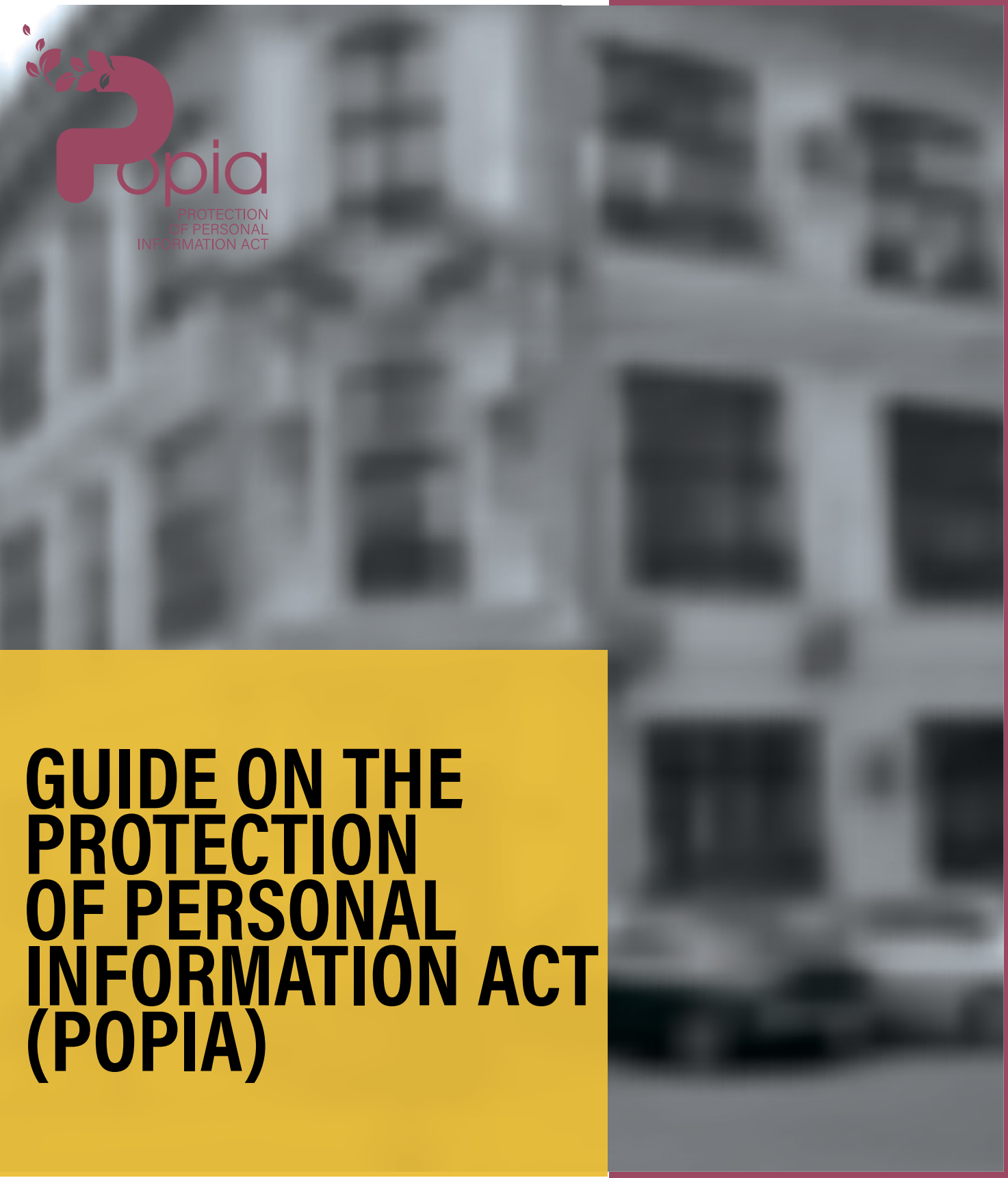


popia
PROTECTION OF PERSONAL INFORMATION ACT

GUIDE ON THE PROTECTION OF PERSONAL INFORMATION ACT (POPIA)

Issued
9 May 2022

SAICA
develop.influence.lead.
THE SOUTH AFRICAN INSTITUTE OF CHARTERED ACCOUNTANTS

develop.influence.lead.

ISBN 978-0-86983-448-0

TABLE OF CONTENTS

TABLE OF CONTENTS

PREFACE

This guide has been developed by the South African Institute of Chartered Accountants (SAICA) and is intended as a summary guideline to members and associates regarding the processing of personal information by public and private bodies.

The Standards and Legal Divisions of SAICA, in association with the Legal Compliance Committee, have prepared the guide.

Every effort is made to ensure that the content of this guide is correct and aligned with legislation as at the date of this guide. This guidance is given to members and associates of SAICA purely to assist them with the subject matter of this guide, however, SAICA does not warrant that this guide deals with every aspect relating to the subject matter. SAICA shall have no liability to any members, associates and/or any third party for any claim of any nature whatsoever which may arise out of the use of and/or reliance on the contents of this guide. Members, associates and/or any third party hereby waive any rights to any claim of any nature whatsoever which may arise out of the use of and/or reliance on this guide, and further indemnifies SAICA against any claim of any nature whatsoever. Members and associates should keep abreast of legislative developments, related guidance issued by regulators and any case law relevant to the subject matter. If there is any conflict between the contents of this guide and the aforementioned legislative developments, related guidance issued by regulators and any relevant case law, members and associates must comply with the latter.

1 INTRODUCTION

The Protection of Personal Information Act 4 of 2013 (POPIA) was assented to on 19 November 2013. However, the substantive provisions of POPIA which place obligations on responsible parties only became enforceable on 1 July 2021.

POPIA sets out the minimum requirements for handling personal information and aims to ensure the protection of personal information processed by either private or public bodies and to regulate the flow of personal information across the borders of the Republic of South Africa.

POPIA needs to be read in conjunction with the regulations, guidelines and any codes of conduct issued by the Information Regulator from time to time. POPIA may also need to be read in conjunction with other legislation that contemplates data protection, such as the Consumer Protection Act 68 of 2008 and the Promotion of Access to Information Act 2 of 2000.

SAICA members and associates must consider the application of POPIA to their business activities. POPIA provides members in business and members in practice with the responsibility for the personal information that they have access to in the conduct of their work.

While this guide focuses on the impact of POPIA on South African entities, it must be noted that there are over 180 jurisdictions with data protection legislation[1] and many more in the process of developing such legislation. One of the more well-known foreign privacy laws is the European Union's General Data Protection Regulation (GDPR), which has extra-territorial jurisdiction (i.e. the GDPR can potentially apply to South African companies). It is important for entities to be cognisant of international data protection laws and perform impact assessments in the jurisdictions in which they operate to determine the impact of these laws on their businesses.

2 PURPOSE OF POPIA

POPIA gives effect to the constitutional right to privacy by safeguarding personal information when it is processed by a responsible party, subject to justifiable limitations. POPIA aims to ensure that the responsible parties act responsibly when dealing with the personal information of the data subject and are held accountable for any abuse or misuse of that personal information.

POPIA regulates the way in which personal information may be processed by POPIA and sets the minimum requirements that a responsible party should adhere to when processing personal information.

It is important to note that POPIA does not prohibit the processing of personal information but rather sets out certain requirements to process personal information lawfully.

POPIA also provides persons with rights and remedies to protect their personal information from processing that is not aligned with POPIA. POPIA also establishes the office of the Information Regulator, who is responsible for enforcement of POPIA through a number of mechanisms.

3 APPLICATION OF ACT

Reference: Section 3

POPIA applies to the processing of personal information which is 'entered into a record' (i.e. recorded) by or for a responsible party. This means that POPIA applies to any record in whatever form or medium in the possession or under the control of a responsible party (whether or not it was created by a responsible party) and regardless of when it came into existence. A record includes any of the following:

- Writing on any material (for example physical documents)
- Information produced, recorded, stored or otherwise derived from any tape recorder, computer equipment, or other device (for example electronic or digital records and tape recordings)
- Books, maps, plans, graphs or drawings
- Photographs, film, negatives, tapes or any other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced
- Any label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means

[1] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide, accessed 9 September 2021.

Where personal information is recorded by non-automated means (i.e. manually) POPIA applies if the record forms part of a filing system or is intended to form part of a filing system.

POPIA applies to the processing of personal information that is entered into a record where the responsible party is domiciled in the Republic of South Africa.

POPIA also has extra-territorial application and applies to the processing of personal information where the responsible party is not domiciled in the Republic of South Africa but makes use of automated or non-automated means in the Republic of South Africa, unless information is only forwarded through the Republic of South Africa.

LETS GET PRACTICAL

An example where POPIA may apply extra-territorially is where a Namibian company engages a South African company to process personal information on its behalf. POPIA would apply because the Namibian company (being the responsible party) is indirectly processing personal information personal information in South Africa.

However, an example of where POPIA will not apply extra-territorially is where a German company is sending personal information of German residents to a Nigerian company which, during the transmission process, is routed through servers which are situated in South Africa. POPIA does not apply where personal information is only forwarded through the Republic of South Africa.

An entity acting in the capacity of an operator, as defined in POPIA, will also have certain responsibilities in terms of POPIA and additional contractual obligations in terms of its contract with the relevant responsible party.

Sections 6 and 7 of POPIA describe the circumstances when POPIA does not apply to the processing of personal information. For example, POPIA does not apply to the processing of personal information in the course of a purely personal or household activity or where personal information has been de-identified and cannot be re-identified again.

4 INTERACTION OF POPIA WITH OTHER LEGISLATION

Reference: Section 3

Section 3(2) states that POPIA will apply to the exclusion of any provision of any other legislation that regulates the processing of personal information and that is materially inconsistent with an object or a specific provision of POPIA, unless other legislation provides for conditions for the lawful processing of personal information that are more extensive than POPIA, in which case the more extensive provisions prevail.

LETS GET PRACTICAL

An example where POPIA and another piece of legislation overlap is in respect of the processing of personal information for direct marketing purposes. In this regard both POPIA and the Consumer Protection Act 68 of 2008 (CPA) regulate direct marketing. However, while section 69 of POPIA specifically regulates direct marketing via electronic communication, the CPA regulates direct marketing more broadly and applies to all forms of direct marketing. Where there is an overlap or contradiction between the provisions of the CPA and POPIA, you must apply the stricter requirement which affords the data subject / consumer the greatest protection. (Please refer to *Annexure B* for a better understanding of the interplay between POPIA and the CPA as it applies to direct marketing.)

It is also important to recognise that POPIA and the Promotion of Access to Information Act 2 of 2000 (PAIA) dovetail in a number of respects, but particularly insofar as the requirement to appoint an information officer, the requirement to maintain a record of processing operations, and the manner in which access to records should be governed.

POPIA cross-references PAIA in several instances, some of which are listed below:

- The definition of 'information officer' of a private body is defined with reference to the definition in PAIA
- Section 17 of POPIA requires that responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 14 or 51 of PAIA (commonly referred to as a PAIA Manual)
- Insofar as the manner of requesting access to personal information records is concerned, POPIA states that the provisions of sections 18 and 53 of PAIA apply
- Section 23(4) of POPIA states that a responsible party may or must refuse, as the case may be, to disclose any information requested in terms of POPIA on the grounds for refusal of access to set out in the applicable sections of PAIA
- Further, POPIA states that the provisions of sections 30 and 61 of PAIA are applicable in respect of access to health or other records

5 PERSONAL INFORMATION

Reference: Section 1

A data subject means the person to whom the personal information relates. A data subject can be a SAICA member, a client, an employee and/or a supplier.

The definition of personal information is very wide and includes information related to:

- An identifiable, living, natural person or
- An identifiable, existing juristic person

Personal information includes, but is not limited to:

- Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, disability, religion, conscience, belief, culture, language and birth of the person
- Information relating to the education or the medical, financial, criminal or employment history of the person
- Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person
- The biometric information of the person
- The personal opinions, views or preferences of the person
- Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence
- The views or opinions of another individual about the person, and
- The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person

LETS GET PRACTICAL

SAICA members will likely process a host of personal information in the context of an employer (including names, employee numbers, ID numbers, health information, tax identification numbers, criminal information, views and opinions of employee performance, biometric information, etc).

SAICA members will also process the personal information of their clients and their employees for the purpose of providing services to clients and for the purpose of conducting its business. Examples of personal information that may be processed for the purpose of providing professional services may include:

- **Identifying numbers (such as employees' income tax numbers, directors' identity numbers, company registration numbers)**
- **Information relating to the financial history of their client and/or their employees (such as salary information of directors/employees or the financial information of the client itself)**
- **Email address and telephone numbers**
- **Correspondence sent by clients that is implicitly or explicitly of a private or confidential nature**

While POPIA does not expressly require members to maintain an inventory of the personal information it processes, it is important for members to have a good understanding of all the personal information that they process in order to comply with many of the conditions set out in POPIA. For example, in order to prepare privacy notices in terms of section 18 of POPIA, members will need to understand the personal information they process, the purpose of processing, whether personal information is transferred to recipients outside of South Africa, etc.

It is recommended that members perform an exercise to identify the personal information they process and to record that information (for example in a personal information inventory).

Members should ensure its inventory is as detailed as possible and clearly maps the flow of personal information (i.e. what information is processed, where personal information is collected from, where it is stored and where it is transferred to). Members should also populate the inventory with other useful information such as the purpose for collection of the specific category of personal information, the lawful basis for such collection and the capacity in which it processes personal information (i.e. in the capacity of a responsible party or an operator).

6 SPECIAL PERSONAL INFORMATION

Reference: Sections 26 to 33

Section 26 of POPIA creates a special category of personal information called 'special personal information'. POPIA prohibits the processing of special personal information unless one of the exceptions in section 27 of POPIA applies.

Special personal information includes personal information concerning the –

- Religious or philosophical beliefs of a data subject
- Race or ethnic origin of a data subject
- Trade union membership of a data subject
- Political persuasion of a data subject
- Health or sex life of a data subject
- Biometric information of a data subject, and/or
- Criminal behaviour of a data subject if such information relates to –
  - Alleged commission by a data subject of any offence, or
  - Any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings

In order to lawfully process special personal information, the responsible party must consider whether any of the exceptions in section 27 applies. These exceptions include that the –

- Processing is carried out with the consent of the data subject
- Processing is necessary for the establishment, exercise or defence of a right or obligation of law
- Processing is necessary to comply with an obligation of international public law
- Processing is for historical, statistical or research purposes:
  - To the extent that the purpose serves a public interest and the processing is necessary for the purpose concerned, or
  - It appears to be impossible or would require a disproportionate effort to ask for consent,

  and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent
- Special personal information has been deliberately made public by the data subject, or
- Provisions of sections 28 to 33, as the case may be, are complied with[2]

7 PERSONAL INFORMATION OF CHILDREN

Reference: Sections 34 and 35

The personal information of children (natural persons under 18 years who are not legally competent without the assistance of a competent person to take any action or decision in respect of any matter concerning himself/herself) may not be processed unless one of the exceptions in section 35 of POPIA is met.

Children's information may only be processed if the processing is –

- Carried out with prior consent of a competent person
- Necessary for the establishment, exercise or defence of a right or obligation in law
- Necessary to comply with an obligation of international public law
- For historical, statistical or research purposes to the extent that –
  - The purpose serves a public interest and the processing is necessary for the purpose concerned, or
  - It appears to be impossible or would require a disproportionate effort to ask for consent,

  and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent
- Of personal information that has been made public by the child with the consent of a competent person

[2] Sections 28 to 33 provide additional exceptions which may apply in order to lawfully process certain categories of special personal information.

8 ARE YOU A RESPONSIBLE PARTY OR AN OPERATOR?

Reference: Section 1, Definitions

POPIA differentiates between a 'responsible party' on the one hand and an 'operator' on the other hand. In this regard:

- A 'responsible party' means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information, and
- An '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

Members need to be aware whether they are acting in the capacity of a responsible party or an operator in respect of each processing activity, as their roles and responsibilities will differ depending on the capacity in which they are processing that personal information. (Please refer to *Annexure C* for guidance which aims to assist you in determining whether you are acting in the capacity of an operator or responsible party in respect of the different processing activities you are performing.)

EXAMPLE ADAPTED FROM INTERNATIONAL GUIDANCE[3]

Company A signs a contract with a payroll company to pay the wages on its behalf. Company A tells the payroll company when the wages should be paid, when an employee leaves or has an increase, and provides all other details for the payslip and payment. The payroll company provides the IT system and stores the employees' personal information. Company A would likely be acting in the capacity of a responsible party whereas the payroll company would likely be acting in the capacity of an operator in relation to these processing activities.

When a member outsources certain processing activities for which they are the responsible party (for example contracting a third party to store physical records on its behalf), the third party will likely be acting in the capacity of an operator. It is important to note that the member shall remain responsible for the lawful processing of that personal information by the operator (notwithstanding the fact that it has been outsourced) and for reasonably ensuring that the operator is and remains compliant with POPIA.

When managing their own business information, for example financial information of the practice, members will be acting as a responsible party, but where services are provided to clients, the decision whether the member is an operator or responsible party would depend on the factual circumstances of the case and whether the member alone, or jointly with the client, determines the purpose of and means of processing personal information.

LETS GET PRACTICAL

Each member should analyse its processing activities and determine the capacity in which it processes personal information by considering the following:

- **What is the purpose of processing personal information in each case?**
- **Who determines the purpose of processing personal information?**
- **Who determines the means for processing personal information?**

[3] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-Processor/what-data-controller-or-data-Processor_en, accessed 9 September 2021.

When professional service providers process personal information in accordance with their own professional obligations (for example in line with the any legislation or professional body rules), they will likely be acting as the responsible party, as they will be determining the purpose and means for processing personal information in order to discharge their professional obligations.

Auditors would typically be viewed as responsible parties, as an audit is performed in terms of specific audit standards (i.e. the client cannot prescribe what and how the information provided to the auditor is utilised, as the auditor must act independently and conduct the audit in accordance with the audit standards that apply to the profession).

EXAMPLE ADAPTED FROM INTERNATIONAL GUIDANCE[4]

Company A hires Audit Firm C to carry out audits of their financial statements and therefore transfers data about financial transactions (including personal information) to Audit Firm C. Audit Firm C processes such data without detailed instructions from Company A.

Audit Firm C decides itself, in accordance with legal provisions and professional rules regulating the tasks of the auditing activities carried out by Audit Firm C (i.e. auditing standards), that the data it collects will only be processed for the purpose of auditing Company A and it determines what data it needs to have, how long the data shall be kept and what technical means to use.

Under these circumstances, Audit Firm C is to be regarded as a responsible party of its own when performing its auditing services for Company A.

If the processing of personal information is performed on behalf of the client by the accountant under a contract setting out what personal information the accountant can and cannot process, the means for processing and the purposes for processing, then the accountant could be processing that personal information in the capacity of an operator.

EXAMPLE ADAPTED FROM INTERNATIONAL GUIDANCE[5]

The qualification of members can vary depending on the context. Where members provide services to the general public and small traders on the basis of very general instructions ('Prepare my tax returns'), then the member will be acting in the capacity of a responsible party. However, a member is employed by a firm and subject to detailed instructions from the in-house accountant, perhaps to carry a detailed audit, then in general, if not a regular employee, she/it will likely be acting in the capacity of an operator because of the clarity of the instructions and the consequent limited scope for discretion. However, this is subject to one major caveat, namely that where they consider that they have detected malpractice which they are obliged to report, because of the professional obligations they owe, they are acting independently as a responsible party.

If the contract is not specific regarding the purpose and means of processing personal information and the accountant is free to complete the service as he/she/it deems appropriate, then the accountant could be processing that personal information in the capacity of a responsible party.

[4] European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (version 2.0), adopted on 07 July 2021.

[5] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"', adopted on 16 February 2010.

9 OBLIGATIONS OF A RESPONSIBLE PARTY

The responsible party is ultimately responsible and accountable for the lawful processing of personal information. The responsible party must ensure that he/she/it meets all the requirements of POPIA and that all measures that give effect to POPIA are complied with at the outset and throughout the processing itself. This responsibility is in no way diminished solely because the processing activity has been outsourced to a third party / operator.

It is important that the responsible party take reasonable steps to assess the risks posed by outsourcing the processing to the relevant third party and implement measures to mitigate or avoid those risks (including entering into an appropriate contract / engagement letter that sets out the mandate of the operator, the security expectations, and the manner in which personal information will be treated by the operator). It is also recommended that privacy assurances be obtained from the third party.

Overview of the responsibilities of the responsible party

A responsible party must –

- Comply with all eight conditions (set out in sections 8 to 35 of POPIA) when processing personal information and implement measures to give effect to those conditions
- Ensure that the rights of data subjects are respected and given effect to
- Not process any special personal information of the data subject or the personal information of children unless an exception in POPIA applies to the processing
- Only perform direct marketing by electronic means where the requirements of section 69 of POPIA have been satisfied (see practical guidance provided in *Annexure B*)
- Ensure there is a lawful basis to transfer personal information outside of the Republic of South Africa
- Not process personal information for a purpose which is incompatible with the original purpose for which the personal information was collected (i.e. further processing) unless the requirements in section 15 of POPIA have been satisfied
- Not make decisions about a data subject which result in legal consequences for him/her/it, or which affects him/her/ it to a substantial degree, where the decision is based solely on the automated processing of personal information intended to provide a profile of the data subject
- Consider whether any of its processing activities require the prior authorisation of the Information Regulator as set out in Chapter 6 of POPIA and, if so, obtain such authorisation before conducting those processing activities
- Maintain a PAIA Manual unless an exemption applies, and
- Designate and register an information officer and, where appropriate, deputy information officer(s).

Where a member processes information for clients it would be advisable to amend their engagement letter setting out the POPIA considerations. See *Annexure D1* for topics to be considered in engagement letters with clients.

10 OBLIGATIONS OF AN OPERATOR

Reference: Sections 1, 19, 20 and 21

An operator or anyone processing personal information on behalf of a responsible party or an operator must –

- Process such information only with the knowledge or authorisation of the responsible party, and
- Treat personal information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties

An operator must also notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

The operator must comply with the specific undertakings specified in the written contract with the responsible party when processing personal information for or on behalf of the responsible party.

POPIA does not specify all privacy provisions that should be agreed but does require that, at a minimum, the responsible party must enter into a written contract with each operator. This requires that the operator should establish and maintain the security measures referred to in section 19 of POPIA. (See *Annexure D2* for topics to be considered in engagement letters with operators.)

LETS GET PRACTICAL

Where a member is processing personal information for a client and it is determined, based on the facts, that the member is acting in the capacity of an operator, then the member must ensure that it only processes personal information with the knowledge or authorisation of the client (being the responsible party). The member must treat personal information it receives as confidential and must not disclose it to any third party unless required by law or in the course of the proper performance of their duties.

The client, as the responsible party, may not waive its responsibilities in terms of POPIA and must comply with the processing conditions, unless exceptions apply. This means that the client must inform data subjects (such as its debtors or employees) that their information is shared with third parties (i.e. the member) and any other information which is required by section 18 of POPIA. The client must also ensure that there is a lawful basis for processing that personal information.

While the responsible party is obliged to ensure there is a written contract governing the processing of personal information by the operator, it is the member's responsibility to implement those measures (including the training of employees) to give effect to the contractual obligations.

Where the member is an operator, it is recommended that the member consider obtaining appropriate indemnities from the responsible party to the effect that the responsible party has determined that there is a lawful basis to perform the processing and that it has notified the data subjects that their personal information is being shared with third parties such as the member.

11 PRIVACY GOVERNANCE STRUCTURE

In order to enforce compliance within an organisation, it is important to establish an appropriate governance structure. This must include the appointment and registration of an information officer and may include the appointment and registration of one or more deputy information officers. In larger firms, it may also require that privacy and security committees or forums be established (or that mandates of existing committees or forums be enhanced to have oversight of privacy matters). In this guide we only consider the requirement to appoint and register an information officer and, where applicable, deputy information officers.

Responsible parties should refer to the Guidance Note on Information Officers and Deputy Information Officers dated 1 April 2021 on the website of the Information Regulator for more detailed information regarding inter alia:

- **Who should be registered as an information officer**
- **The duties of the information officer**
- **The designation of deputy information officers and delegation of authority by the information officer to deputy information officers**
- **Training requirements**
- **The procedure to register information officers**

Information officer

Reference: Section 55 and Regulation 4

Who is the information officer of a private company?

Every responsible party is required to appoint an information officer and register that information officer with the information regulator.

'Information officer' has the same meaning as that contained in PAIA and will be, 'by default', the head of a private body, the chief executive officer, or an equivalent officer. POPIA provides that the information officer be the chief executive officer of the organisation or someone with an equivalent rank or function.

It is also possible for another person to act in the capacity of the information officer if that person is duly authorised by that CEO. Such authorisation must be in writing and can be withdrawn at any point. The information officer does not relinquish the responsibility for and ability to exercise the duties of an information officer by virtue of having delegated the authority.

Duties and responsibilities of an information officer

The duties and responsibilities of an information officer are described in section 55 of POPIA and include:

- The encouragement of compliance with the conditions of lawful processing of personal information
- Ensuring compliance of the organisation with the provisions of POPIA
- Dealing with requests made to the organisation as per POPIA
- Working with the Regulator in respect of investigations
- Complying with any additional responsibilities that may be prescribed

The POPIA Regulations further require that information officers must ensure that:

- A compliance framework is developed, implemented, monitored and maintained
- A personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information. (An example of a template report to be compiled following an impact assessment is included in Annexure G)
- A PAIA Manual is developed, monitored, maintained and made available
- Internal measures are developed together with adequate systems to process requests for information or access thereto, and
- Internal awareness sessions are conducted regarding the provisions of POPIA, regulations made in terms of POPIA, codes of conduct, or information obtained from the Regulator.

It is important to note that this section is applicable to all public and private bodies that process information. If an information officer is not appointed, the CEO would be the information officer by default.

Information officers must take up their duties in terms of POPIA only after the responsible party has registered them with the Information Regulator.

Designation and delegation of deputy information officers

Reference: Section 56

It is not mandatory for all organisations to appoint deputy information officers – instead the organisation should consider whether the appointment of one or more deputy information officers is necessary to drive POPIA compliance within the organisation, having regard to the size, structure and complexity of the organisation.

In this regard section 56 of POPIA makes provision for an organisation to appoint of one or more deputy information officers, as is necessary, to support the information officer in discharging his/her responsibilities. However, any power or duty conferred or imposed on an information officer by POPIA can be designated to a deputy information officer.

The delegation of the powers to the deputy information officer must be in writing and can be withdrawn at any time. It does not prohibit the person who delegated such powers and duties from exercising the powers or performing the duties concerned himself/herself.

An information officer retains the accountability and responsibility for the functions delegated to the deputy information officer.

12 EIGHT CONDITIONS FOR THE LAWFUL PROCESSING OF PERSONAL INFORMATION

Reference: Sections 8 to 25

POPIA does not prohibit the processing of personal information but rather states that when personal information is processed it must be processed lawfully in accordance with the requirements of POPIA.

POPIA obliges responsible parties to comply with eight conditions of POPIA, as well as additional requirements which are discussed in Parts 14 to 17 of this guide.

The POPIA requirements apply in every instance of you processing personal information of data subjects, whether you are processing the personal information of employees, suppliers, debtors, creditors, clients or other third parties (such as visitors to a premises).

POPIA lists the eight conditions for the lawful processing of personal information which need to be adhered to by all responsible parties, including SAICA members.

SAICA members should also be aware that POPIA has additional requirements which need to be adhered to when performing direct marketing, international transfers, automated decision-making, developing directories and/or performing processing activities which are subject to the prior authorisation of the Information Regulator, etc.

12.1 Condition 1: Accountability

Reference: Section 8

The obligation to comply with each of the eight conditions for the lawful processing of personal information falls on the responsible party. The responsible party must comply with POPIA and should be able to demonstrate such compliance.

The responsible party must be proactive and ensure that all reasonable measures are taken to comply with the eight conditions of POPIA when first determining what the personal information is going to be used for (i.e. the purpose) and the means of processing the personal information. This obligation applies throughout the course of processing that information.

It is not possible to contract out of the obligations placed on the responsible party (for example by outsourcing the processing of personal information to a third party). In fact, POPIA requires that the responsible party undertake additional security measures where the responsible party does use a third party to process personal information on its behalf. (See Part 1.9 of this guide regarding mitigation measures to be considered when outsourcing processing to a third party.)

Accountability is not a tick-box exercise – the measures that should be implemented to demonstrate accountability for compliance will differ from one organisation to another.

Members will act in the capacity of a responsible party in relation to some or all of its processing activities and therefore should implement control measures to minimise the risk of non-compliance with POPIA.

These control measures could include:

- **Maintaining a personal information inventory so that you have a good understanding of your personal information processing activities across the firm (i.e. a personal information inventory should clearly record your processing activities, purpose(s) for processing, types of personal information needed to achieve that purpose, lawful basis for processing, source of personal information, storage places(s), transfer of personal information, retention periods, etc)**
- **Establishing an appropriate privacy and security governance structure including appointing an information officer (and where necessary deputy information officer(s)) with the necessary skills, expertise and capacity to drive POPIA compliance with the firm**
- **Developing appropriate policies and procedures to support compliance by employees the examples of policies which**

may need to be developed depending on nature of the firm and its processing activities may include the following:

- **Privacy policy**
- **Information classification and handling policy**
- **Acceptable usage policy**
- **Access management control policy and procedure**
- **Antivirus and patch management procedure**
- **Backup and restoration policy and procedure**
- **Bring your own device (BYOD) policy**
- **Change management policy and procedure**
- **Clean desk and clear screen policy**
- **Data loss prevention (DLP) policy**
- **Information incident management policy and procedure**
- **Information security policy**
- **Information transfer policy**
- **Mobility and remote working policy**
- **Vulnerability and penetration testing policy and procedure**
- **Retention and destruction policy (including retention schedules)**

- **Ensuring existing and new employees are appropriately trained and understand their roles and responsibilities in terms of POPIA (and any additional contractually agreed obligations)**
- **Ensuring written contracts are in place with all operators and other third parties who have access to personal information**
- **Ensuring you stay abreast of any changes to POPIA as well as any regulations and codes of conduct which are issued from time to time and that your processes adjust accordingly**
- **Implementing reasonable and appropriate security measures**
- **Implementing processes to detect, contain and report personal information breaches if they happen**
- **Apply principles of International Guidelines, where appropriate, such as the principle of 'privacy by design and default' when implementing new processes or systems**

12.2 Condition 2: Processing limitation

Reference: Sections 9 to 12

Lawfulness of processing

It is imperative for the responsible party to ensure that the processing of personal information is lawful and done in a manner that is reasonable and does not infringe on the privacy of the data subject. This means, *inter alia*, that the responsible party must:

- Have a lawful basis or lawful justification for processing the personal information
- Not collect or otherwise process personal information, special personal information or a child's personal information where it would be unlawful to do so
- Not act in a manner which is unlawful in terms of POPIA or which is contrary to the spirit and purpose of POPIA

Members should note that this requirement is closely linked to section 11(1), which sets out the various lawful justifications which may allow a responsible party to process personal information.

Members should also note that there are more limited lawful justifications when processing special personal information and/or a child's personal information. Refer to Parts 6 and 7 of this guide for more information about how to ensure that you process these more sensitive categories of personal information lawfully.

Minimality

Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive. In other words, organisations should only collect the minimum information required for the specific purpose.

If an organisation is storing personal information of an individual or company, it should only hold that personal information to achieve the purpose for which it was originally collected (for example for the provisions of the agreed professional services to the client). The organisation should not hold any more personal information than is necessary to achieve that purpose.

Do not collect personal information simply because it may be valuable in the future.

To determine whether you are collecting and holding the minimum personal information necessary, members need to first be clear about why they need the information. You should not collect more information than needed to achieve that purpose and should ensure that you do not request or store irrelevant or unnecessary personal information.

Where a client / data subject sends you more personal information that you requested and require, you should communicate this to the client / data subject and agree whether the personal information will be returned (only applicable to physical records), destroyed (applicable to physical and electronic records), or retained with the explicit consent of the data subject.

Consent, justification and objection

Personal information cannot be processed unless there is at least one lawful justification which allows the processing of personal information. Section 11 of POPIA does not give preference to any of the lawful justifications for processing personal information as long as there is at least one lawful justification for the processing. Members should consider all lawful justifications and determine which lawful basis is the most

appropriate. It is also recommended that members maintain a record which evidences the lawful basis upon which it relies to perform the processing activity. Annexure E can be used to determining and recording whether there is a lawful basis for a particular processing activity. Section 11(1) sets out a number of lawful justifications for processing personal information. Section 11 states that personal information may only be processed if at least one of the follow justifications apply:

- The data subject, or a competent person where the data subject is a child, consents to the processing

LETS GET PRACTICAL

In order for consent to be legitimate it must be a voluntary, specific and informed expression of will in terms of which the permission is given for the processing of personal information.

It is not recommended that members rely on tacit consent / opt-out consent, 'bundled consent' (where consent is bundled with other terms and conditions) or 'blanket consent' (where consent it given in respect of any and all processing of personal information).

While consent is one of the most well-known lawful justifications, it is not preferred over the other lawful justifications set out in section 11(1) of POPIA. In fact, based on international guidance, there are certain instances where consent would be an inappropriate justification for processing personal information. For example, based on international guidelines, it is not recommended that you rely on employees' consent where there is an alternative legal justification for processing personal information, as it can be argued that the employee's consent was not voluntary due to the unequal bargaining power between the employer and employee.

The responsible party bears the onus of proving that it has obtained the consent of the data subject to process the personal information. It should also be borne in mind that POPIA allows the data subject to withdraw his/her/its consent at any time. Accordingly, wherever consent is relied upon, it is important that the responsible party implement effective consent management processes which ensure that it is able to:

- **Evidence that the data subject exercised informed consent (i.e. that the data subject was provided with sufficient information to make an informed decision regarding the processing of his/her/its personal information – this can be achieved by providing the data subject with an appropriate privacy notice)**
- **Evidence that valid consent was provided (whether such consent was obtained in writing or electronically). Verbal consent is generally not recommended unless it is recorded or it is an emergency situation, and**
- **Give effect to the withdrawal of consent (i.e. by stopping the processing of personal information until another lawful basis for processing can be established and communicated to the data subject). Importantly, the lawfulness of the processing of personal information before such withdrawal of consent will not be affected**

- Processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party (for example processing is necessary for the professional services firm to perform its in terms of its contract with the client, or necessary to perform its obligations to the employee in terms of the employment contract)
- Processing complies with an obligation imposed by law on the responsible party (for example the storage of personal information relating to historical tax information and advice given)
- Processing is necessary for pursuing the legitimate interest of the data subject (for example processing of beneficiaries' personal information to administer pension benefits)*
- Processing is necessary for the proper performance of a public law duty by a public body (this only applies where the responsible party has a public law duty or is itself a public body),* or
- Processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied (for example to reasonably secure its physical premises, IT security, fraud prevention, intra-group transfers etc)*

LETS GET PRACTICAL

Members should not assume that the justification of legitimate interest will apply as a 'catch all' where no other lawful basis exists. When relying on this lawful basis, members, where they are responsible parties, should consider documenting the reason they believe this justification is appropriate and can be relied on. Based on international guidance three pertinent questions should be considered in determining whether you can rely on this legal justification:

- **Purpose test –** Is the purpose you are pursuing considered a legitimate interest of the responsible party / third party?
- **Necessity test –** Is the processing necessary to achieve that purpose or could the legitimate interest be achieved in a less intrusive manner?
- **Balancing test –** Does the individual's interest override the legitimate interest of the responsible party / third party, as applicable?

***Objections**

A data subject may object, at any time, to the responsible party, to the processing of personal information on reasonable grounds relating to his/her/its particular situation, unless legislation otherwise provides for such processing. If a data subject has objected to the processing of the personal information on reasonable grounds, the responsible party may no longer process the personal information.

LETS GET PRACTICAL

Members that operate a website accessible to members of the public will need to understand what cookies are and what they are being used for. A cookie is a small text file that is downloaded onto a computer or smartphone, for example when the user accesses a website. There are different types of cookies, but the most well-known categories are:

- **Strictly necessary cookies –** These cookies are essential to ensure that the visitor can navigate and use certain functions of the website. Without them, essential parts of the website cannot be used. Accordingly, these cookies are always activated by companies and typically consent is not required based on international guidance.

LETS GET PRACTICAL

- **Functional cookies –** These cookies typically enable the website to store information such as the username, region or language selection and to offer the user improved and personalised functions based on this information. These cookies typically support in ensuring that the website is designed for optimum user-friendliness. Functional cookies are also used, for example, to activate the functions the user desires.
- **Targeting/marketing cookies –** These cookies are typically used to gather information from you in order to display content or advertisements that is more relevant to the user and adapted to his interests. These cookies may also be used to measure and control the effectiveness of campaigns. For example, they register whether a website has been visited or not, as well as which content has been used. This information is used to create an interest profile so that only content that is interesting for the user is displayed. Withdrawing consent to marketing cookies does not mean that the user will see or receive less content as a result, rather it means that the content the user sees and receives is not tailored to his/her individual needs.
- **Performance cookies –** These cookies typically function by collecting data on user behaviour (for example gathering information on how user uses a website, which pages are visited most frequently, if there are error messages). On this basis, the website is adjusted to the general user behaviour in terms of content and functionality. Performance cookies are generally used to improve the performance of the website and to tailor the online experience to the needs of the users.

While POPIA does not provide express guidance regarding the lawful use of cookies, it will be important to consider the conditions of POPIA and apply these to cookies. Some tips would be to:

- **Inform data subjects** that the website uses cookies (for example by ensuring a banner is prominently displayed on the webpage visited by the data subject)
- **Provide clear and comprehensive information** regarding what cookies are doing, the purpose(s) for which the information is being used, and the manner in which the data subject can provide or withdraw consent to the use of cookies
- **Obtain the data subject's consent** to store a cookie on their device where the cookie is not essential / strictly necessary to provide the service

Members should also be aware that there are numerous web tracking technologies that do not rely on cookies to track behaviour and should investigate whether such technologies are being used by their company.

Collection directly from the data subject

Personal information is required to be collected directly from the data subject. There are, however, exceptions to this requirement, namely that personal information may be collected indirectly (from an alternative source) if:

- The information is contained in or derived from a public record (for example records of the Deeds Office or the Companies and Intellectual Property Commission)

- The information has deliberately been made public by the data subject (directors' remuneration submitted to the Companies and Intellectual Property Commission as part of the annual financial statements or information contained on the data subject's website)
- The data subject has consented to the collection of the information from another source (or where the data subject is a child, the competent person has consented to the collection from another source)
- Collection of the information from another source would not prejudice a legitimate interest of the data subject
- Collection of the information from another source is necessary –
  - To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences
  - To enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act 34 of 1997
  - Tor the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated
  - In the interests of national security, or
  - To maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied (see SAICA Let's get practical above regarding reliance on legitimate interests)
- Compliance would prejudice a lawful purpose of the collection, or
- Compliance is not reasonably practicable in the circumstance

When acting in the capacity of a responsible party, members will need to comply with the principles of collection when discharging their professional responsibilities. In this context, audit members often collect personal information of data subjects (such as employees, directors or debtors) indirectly from the client. Obtaining the consent of the data subject for the collection of personal information from the client is often not practical as the member does not have a direct relationship with the data subject and/or it is not reasonably practicable to obtain consent due to the number of data subjects involved. Indirect collection could nevertheless be permissible on the basis that one or more of the exceptions apply:

- **The personal information collected is contained in or derived from a public record**
- **The collection of the information from the client would not prejudice a legitimate interest of the data subject**
- **The collection of the information from another source (i.e. the client) is necessary to maintain the legitimate interests of the member (being the responsible party), or**
- **Compliance is not reasonably practicable in the circumstances**

12.3 Condition 3: Purpose specification

Reference: Sections 13 and 14

Collection for a specific purpose

Personal information can only be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.

Members should document the purposes for which they process personal information at the outset. This will assist members in:

- **Ensuring its privacy notices correctly reflect the purpose(s) for which personal information is collected, and**
- **Avoiding the unlawful processing of personal information which is incompatible with the original purpose (i.e. further processing)**

Responsible parties must be open and transparent with data subjects regarding the purpose(s) that personal information will be used. It is therefore important that when personal information is collected, responsible parties inform data subjects what the personal information is going to be used for.

This obligation is closely linked to the obligation in section 18 of POPIA which obliges responsible parties to provide data subjects with a privacy notice to ensure that the data subject is aware of pertinent information regarding the responsible party's processing activities.

Retention, destruction and restriction of records

Restriction on retention

Even where a responsible party has collected and used personal information lawfully, that does not mean it can keep that personal information indefinitely. POPIA require responsible parties to delete personal information that is no longer necessary for achieving the purpose for which the personal information was originally collected or subsequently processed.

However, POPIA allows responsible parties to retain personal information records for longer than is necessary for achieving its purposes if –

- Retention is required or authorised by law
- The responsible party reasonably requires the record for lawful purposes related to its functions or activities
- Retention is required by a contract between the parties, or
- The data subject (or competent person, where the data subject is a child) has given consent to the retention of the record

Retention for historical, statistical or research purposes

Records of personal information may also be retained for periods longer than is necessary for historical, statistical or research purposes, but only if the responsible party has established appropriate safeguards against the records being used for any other purpose(s).

Mandatory retention of records used to make a decision about the data subject

Where a record of personal information has been used by the responsible party to make a decision about the data subject –

- The responsible party must retain the record for such period as may be required by law or a code of conduct, or
- Where there is no law or code of conduct prescribing the retention period, then the record must be retained for a period which will afford the data subject a reasonable opportunity (taking all considerations relating to the use of the persona information into account) to request access to the record

LETS GET PRACTICAL

POPIA does not expressly require that organisations implement a formal retention policy or retention schedule. However, such policies and schedules can support your organisation in complying with the retention and destruction obligations specified in POPIA. Policies and schedules support employees in understanding their obligations as it pertains to retention and destructions and promotes a consistent application of retention principles.

Small organisations undertaking occasional low-risk processing may not need to formally document their retention practices in a policy; however, they will need to implement appropriate procedures to ensure that they –

- **Regularly review the records they retain, and**
- **Destroy, delete or de-identify those which they are no longer authorised to retain**

It is also good practice to maintain a record of the company's destruction activities.

LETS GET PRACTICAL

Destruction, deletion, or de-identification of personal information that is no longer required may present organisations with many challenges in light of the vast amount of legislation that requires records to be kept for differing periods of time.

The SAICA Guide on the Retention of Records provides guidance in terms of the requirements of various legislation's document retention requirements.

Members would need to consider the retention of client documents used in the provision of services.

In the case where a tax practitioner provided a tax opinion, the law would not set out a requirement to retain the documents as well as the client information used to prepare the opinion. The tax practitioner would need to consider by when the information would no longer be required to be retained. If the tax practitioner wants to retain the information for a longer period, they would need the consent of the client or retention would be prescribed by the contract between the tax practitioner and the client.

Destruction

Destruction, deletion or de-identification of a personal information record must be done as soon as reasonably practicable after the responsible party is no longer authorised to retain the record in terms of POPIA. The destruction or deletion of a record must be done in a manner that prevents reconstruction in an intelligible form.

When a responsible party is no longer authorised to retain a record of personal information, it must ensure that all physical and electronic versions of the record (including back-ups of the record) are destroyed, deleted or de-identified.

When it comes to physical records, shredding is usually a quick, easy and cost-effective manner of destroying records. If you use a shredding service (i.e. outsource shredding), you should use a reputable company, witness the shredding (if practical) and obtain a certificate of destruction.

Insofar as electronic records are concerned, you should be aware that systems often have back-ups and background storage. You should seek specialist IT advice to ensure that personal information records are securely deleted or destroyed when you are no longer authorised to retain those records.

Remember that unused assets (old computers, hard drives, USBs, mobile phones) may contain personal information records and any records on these devices should be dealt with in accordance with POPIA.

Restriction

The processing of personal information must be restricted if –

- Its accuracy is contested by the data subject
- The information has been retained for the purpose of proof
- The processing is unlawful but the data subject opposes its destruction or deletion and requests the restriction of its use instead, or
- Where the data subject requests to transmit the personal information into another automated processing system

The responsible party must inform the data subject before lifting the restriction on processing.

Except for storage, personal information may only be processed –

- For the purpose of proof, or
- With the data subject's consent (or with the consent of a competent person in respect of a child), or
- For the protection of the rights of another natural or legal person, or
- If such processing is in the public interest

12.4 Condition 4: Further processing limitation

Reference: Section 15

Further processing to be compatible with purpose of collection

Personal information can only be further processed (i.e. processed for an additional or different purpose) if the further processing is in accordance or compatible with the original purpose for which the personal information was collected.

LETS GET PRACTICAL

Section 13 of POPIA requires that responsible parties collect personal information for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party. However, POPIA does not altogether ban the processing of personal information for new or additional purposes which the responsible party did not originally anticipate. POPIA simply requires that the new purpose of processing is in accordance or compatible with the original purpose that the personal information was collected.

Where members wish to process personal information for a new or additional purpose which is different from the original purpose of collection, they should assess whether that new or additional purpose is compatible and document the outcome of this assessment.

In order to assess whether the further processing is compatible with the purpose of the collection the following factors need to be considered:

- The relationship between the purpose of the intended further processing and the collection thereof
- The nature of the personal information concerned
- The consequences of the intended further processing for the data subject
- The manner in which the information has been collected, and
- The contractual rights and obligations between the parties

POPIA states that the further processing of personal information is not considered incompatible with the purpose of collection if –

- The data subject (or competent person where the data subject is a child) has consented to the further processing of personal information
- The personal information is available or derived from a public record
- The personal information has deliberately been made public by the data subject
- Further processing is necessary to –
  - Avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences
  - To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act 34 of 1997
  - For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated, or
  - In the interest of national security
- Further processing is necessary to prevent or mitigate a serious or imminent threat to public health or public safety or the life or health of another individual
- Personal information it is used for historical, statistical or research purposes provided that the responsible party ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form, or
- The further processing of personal information is in accordance with an exemption granted in terms of section 37 of POPIA

Generally, if the new purpose would be unexpected by the data subject or have a material impact on the data subject, it is unlikely that further processing will be considered compatible with the original purpose, and it should not be done.

Although POPIA does not explicitly require that the data subject be made aware of the further processing, it is recommended that a responsible party inform data subjects of this new purpose, where possible.

Members should also be cognisant of the lawful basis for originally collecting and processing personal information. If the lawful basis relied on was consent, then it is recommended that you obtain the data subject's voluntary, informed and specific consent for such further processing.

12.5 Condition 5: Information quality

Reference: Section 16

Quality of information

The responsible party must take 'reasonably practicable steps' to ensure that the personal information is complete, accurate, not misleading and updated where necessary having regard to the purpose for which the information was collected.

Where you collect personal information indirectly from a source other than the data subject, you should consider the reliability of the source and take even more care where the personal information could have serious consequences for the data subject.

- **Ensure that personal information is accurately captured at the time it is collected and, if possible, record the source of personal information.**
- **Take proactive measures to ensure that personal information is kept accurate and up to date if you use the personal information for a purpose that relies on it remaining current.**
- **Carefully consider any challenges to the accuracy of personal information that are raised by the data subject and, where records are inaccurate, incomplete or misleading ensure you take corrective action across your records.**
- **If you obtain any new information which suggests the personal information you have on record is wrong or misleading, you should interrogate the accuracy of the affected records and take steps to erase, update or correct them in light of that new information.**
- **Where personal information consists of an opinion, then the records must make clear that it is an opinion and, where appropriate, identify whose opinion it is. It is also good practice to add a note where the data subject has challenged an opinion, the reasons for challenging the opinion and a reason why the opinion remains unchanged (if applicable).**

12.6 Condition 6: Openness

Reference: Sections 17 and 18

Documentation

A responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 14 or 51 of the Promotion of Access to Information Act 2 of 2000 (PAIA). This document is colloquially referred to in business as a 'PAIA Manual'. Where you already have PAIA Manual, you must ensure it has been updated with regard to the amendments that POPIA has effected to PAIA.

The contents of the PAIA Manual are detailed in PAIA. However, from a POPIA perspective, the PAIA Manual must include –

- The purpose of the processing
- A description of the categories of data subjects and of the information or categories of information relating thereto
- The recipients or categories of recipients to whom the personal information may be supplied
- Planned transborder flows of personal information, and
- A general description allowing a preliminary assessment of the suitability of the information security measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information which is to be processed

LETS GET PRACTICAL

The contents of the PAIA Manual as it pertains to POPIA includes very similar information as required in terms of section 18 of POPIA. It is therefore important that the PAIA Manual and privacy notices developed in terms of section 18 be aligned and regularly updated to reflect the responsible party's processing activities.

The PAIA Manual must be made available:

- **On the responsible party's website (if it has one)**
- **At the principal place of business of the private body for public inspection during normal business hours**
- **To any person upon request and upon the payment of a reasonable amount, and**
- **To the Information Regulator upon request**

It is also recommended that the responsible party's privacy notice be published prominently on its website or intranet site in the case where a separate privacy notice is developed for employees.

Notification to data subject when collecting personal information

Content of privacy notice

Section 18 of POPIA obliges the responsible party to be transparent with data subjects regarding its intended processing activities. Section 18(1) prescribes the minimum information that data subjects should be made aware of. In this regard, if personal information is collected, the responsible party must take reasonably practicable steps to notify the data subject of –

- The personal information being collected as well as the source if the personal information is not collected directly from the data subject
- The name and address of the responsible party
- The purpose for the collection of personal information

- Whether the supply of personal information is voluntary or mandatory
- Consequences of failure to provide personal information
- Any law authorising or requiring the collection of the personal information
- If applicable, the fact that the responsible party intends to transfer personal information outside the Republic of South Africa or to an international organisation and the level of protection afforded to the personal information by the foreign country or international organisation, and
- Any further information which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable such as –
  - Recipient or category of the recipients of the personal information
  - Nature or category of the personal information
  - The existence of the right of access to personal information collected
  - The existence of the right to rectify personal information collected
  - The existence of the right to object the processing of personal information in certain circumstances, and
  - The existence of the right to lodge a complaint to the information regulator as well as the contact details of the Information Regulator

Timing of privacy notice

Reasonable steps must be taken to ensure that the data subject is aware of the above information –

- Before the information is collected if the personal information is being collected directly from the data subject, or
- Before the information is collected or as soon as reasonably practicable after the information has been collected if the personal information is collected indirectly from another source

It will not be necessary for the responsible party to discharge its notification obligations to the same data subject again if the responsible party has previously taken reasonable steps to ensure that the data subject is aware of the information required by section 18(1). This relaxation only applies if the responsible party is –

- Collecting the same personal information or information of the same kind, and
- If the purpose of collection remains the same

In order to ensure compliance, the information may be provided in the agreement or application form (if such an instrument is used).

It is interesting to note that POPIA makes it clear that compliance with the condition of openness in certain instances is NOT required.[7]

7 It is not necessary for a responsible party to comply with the transparency requirements of section 18 of POPIA if –

- The data subject, or a competent person where the data subject is a child, has provided consent for the non-compliance
- Non-compliance would not prejudice the legitimate interests of the data subject
- Non-compliance is necessary –
  - To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences
  - To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act 34 of 1997
  - For the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated, or
  - In the interests of national security
- Compliance would prejudice a lawful purpose of the collection

Where personal information is not collected directly from the data subject and the recipient is collecting the information from a responsible party in terms of a mandate, the mandate between the recipient and the responsible party governs the responsibilities of the recipient. The recipient is regarded as an operator as defined in POPIA. The mandate must align to the operator's responsibilities in terms of POPIA. An example of such an instance is where a member in practice receives the information of the client's debtors as part of an accounting or audit engagement, governed by an engagement letter. The member has no direct relationship with the debtors of the client. The engagement letter, as the mandate, must set out the expectation of the client (responsible party) vis-à-vis the member re the information of the debtors. The client as the responsible party may not waive its above responsibilities in terms of POPIA and must comply with the condition of openness, unless one of the exceptions apply. The client may inform its debtors that their information is shared with members and auditors and that the processing of the information is governed by appropriate clauses as set out in the engagement letter with the member. The engagement letter should as a minimum deal with the member's obligations as the operator.

12.7 Condition 7: Security safeguards

Reference: Sections 19 to 22

Integrity and confidentiality of personal information

Section 19 of POPIA requires the responsible party to secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent –

- Loss of, damage to or unauthorised destruction of personal information, and
- Unlawful access to or processing of personal information

In order to implement appropriate security safeguards to secure the integrity and confidentiality of personal information, section 19(2) of POPIA requires that the responsible party must take reasonable measures to –

- Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control
- Establish and maintain appropriate safeguards against the risks identified
- Regularly verify that the safeguards are effectively implemented, and
- Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards

Generally accepted information security practices

Section 19(3) of POPIA further obliges the responsible party to have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

- Compliance is not reasonably practicable in the circumstances of the particular case, or
- The information will not be used in a form in which the data subject may be identified, or
- The information will be used for historical, statistical or research purposes

LETS GET PRACTICAL

POPIA does not define the minimum security measures that members should implement. The security measures that are appropriate differs from one firm to another. To determine what is appropriate a firm should perform a security risk assessment, considering processing activities and any third parties that may be involved. The security risk assessment should consider the nature or information assets (including personal information), where it is stored, transmitted or processed and what the potential threats are. The security measures implemented should be appropriate to the firm's circumstances as well as the risks reasonably identified during the security risk assessment.

Security safeguards should involve a combination of technical measures (such as firewalls and anti-malware) and organisational measures, including the implementation of policies and procedures and ensuring employees are appropriately trained. Organisations should consider the generally accepted information security practices and procedures which apply to the industry or apply in terms of professional rules and regulations

Once the firm has determined what security measures are appropriate and have implemented those measures, it is important to periodically assess the effectiveness of those controls and improve them where there are deficiencies. This type of testing may require the support of information security experts or suitable independent assurance provider.

(Please refer to *Annexure F* for some information of some basic security measures to be considered by small low-risk firms.)

Information processed by an operator

Where the responsible party engages with an operator to process personal information on its behalf, the responsible party has a duty to ensure that the third party establishes and maintains the security measures referred to in section 19 of POPIA. POPIA requires that the responsible party enter into a written contract with the operator to contractually oblige the operator to comply with section 19. (Please refer to Annexure D2 for examples of the topics that may be included in contracts with operators.)

LETS GET PRACTICAL

The responsible party remains responsible and accountable even when it has outsourced the processing to an operator. To mitigate the privacy risks posed by operators, responsible parties should –

- **Only engage with an operator that provides sufficient assurances about its security environment**
- **Ensure that the written contract with the operator requires the operator to implement the security measures specified in section 19 of POPIA that apply to the responsible party**
- **The contract is clear regarding the processing mandate of the operator**
- **The contract details any additional personal information handling requirements that apply**
- **The contract restricts international transfers and further outsourcing of processing activities except with the prior written consent of the responsible party**

LETS GET PRACTICAL

- **The contract obliges the operator to make available all information necessary to demonstrate compliance with POPIA and allows the responsible party (or an independent third party) to perform a privacy audit**
- **Is clear regarding the manner in which suspected personal information breaches should be reported to the responsible party, and**
- **Negotiate indemnity or penalty clauses where there is non-compliance with the privacy obligations contractually agreed and such non-compliance results in damages to the responsible party**

(Please refer to *Annexure D2* for additional topics that could be included in a contract with operators.)

Notification of security compromises

Section 22 of POPIA governs the notification requirements of the responsible party where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person. These obligations are dealt with in Part 18 of this guide.

Section 21(2) of POPIA obliges operators to notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

LETS GET PRACTICAL

Members (whether acting in the capacity of a responsible party or of an operator) should ensure that they have reasonable processes in place to detect and contain an information security breach (which includes, but is not limited to, a cyber incident). Members (whether acting the capacity of a responsible party or of an operator) should also implement formal plans regarding the manner in which a data breach will be handled.

Where the member is a responsible party, he/she/it must be fully aware of the measures that the operator will take to prevent and detect attempts to unlawfully access the personal information as well as actual data breaches. The operator must immediately inform the responsible party of suspected breaches. The agreement between the operator and the responsible party should make provision for the process to be followed where there is a suspected data breach and must enable the responsible party to investigate the data breach.

The responsible party is responsible for reporting suspected breaches to the information regulator and the data subject. The responsible party must further be in a position to document both the nature of the breach, the controls that were compromised and the data that was exposed by the breach.

12.8 Condition 8: Data subject participation

Reference: Sections 23 to 25

Overview of the rights of the data subject

In terms of POPIA, data subjects have a number of rights which must be respected by the responsible party. These include the –

- Right to request access to personal information records
- Right to request the correction or deletion of personal information records
- Right to object to the processing of personal information in certain instances
- Right to object to the use of personal information for direct marketing purposes
- Right to be notified that personal information about him, her or it is being collected
- Right to be notified that his, her or its personal information has been accessed or acquired by an unauthorised person
- Right to withdraw consent which has previously been provided
- Right not to be subjected to unlawful automated decision making, and
- Right to lodge a complaint with the information officer or with the Information Regulator

However, we only consider the rights of access, correction and deletion in this part of the guide, as these are specified under condition 8 of POPIA.

Access to personal information

Rights

Section 24 of POPIA gives a data subject two distinct rights regarding access to their personal information. In both cases POPIA obliges the data subject to provide adequate proof of identity. In this regard the data subject has the right –

- To request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject
- To request a record (i.e. a copy of the record) or a description of the personal information held by the responsible party about the data subject, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the personal information

Obligations of the responsible party

On receipt of such a request, the responsible party –

- Is obliged to consider and respond to the request within a reasonable time
- May charge a prescribed fee to provide access to a record
- Must respond in a reasonable manner and format,
- Must respond in a form that is generally understandable, and
- Should inform the data subject of his/her/its right to request the correction of personal information if personal information is communicated to a data subject

Payment of fees

If the responsible party requires the data subject pay a fee for services provided to the data subject (as contemplated above) to enable the responsible party to respond to a request, the responsible party must give the applicant a written estimate of the fee before providing the services and may require the applicant to pay a deposit for all or part of the fee.

Grounds for refusal

A responsible party may or must refuse (as applicable) access to information based on the grounds for refusal of access as contained in Chapter 4 of PAIA. The grounds for refusal that apply to the records of private entities are detailed in sections 63 to 69 of PAIA and include the following:

- Mandatory protection of privacy of third party who is natural person (section 63 of PAIA)
- Mandatory protection of commercial information of third party (section 64 of PAIA)
- Mandatory protection of certain confidential information of third party (section 65 of PAIA)
- Mandatory protection of safety of individuals, and protection of property (section 66 of PAIA)
- Mandatory protection of records privileged from production in legal proceedings (section 67 of PAIA)
- Commercial information of private body (section 68 of PAIA)
- Mandatory protection of research information of third party, and protection of research information of private body (section 69 of PAIA)

LETS GET PRACTICAL

It is important to consider the detailed grounds for refusal contained in PAIA, as some of the grounds for refusal are mandatory whilst others are voluntary. The grounds are also subject to conditions and exceptions which need to be considered in determining whether the data subject's request for access can be given effect to or not.

PAIA contains additional protections where a data subject requests access to health records (see sections 30 and 61 of PAIA for more information).

If a request for access to personal information is made to a responsible party and part of that information may or must be refused, every other part must be disclosed to the data subject. (Section 23(5) of POPIA.)

Correcting personal information under POPIA

Rights

In terms of section 24, a data subject may, in the prescribed manner, request a responsible party to:

- Correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully, or
- Destroy or delete a record of personal information about the data subject that the responsible party is *no longer authorised to retain*

Obligations of responsible party

On receipt of such a request and following an assessment of the legitimacy of the request, the responsible party must as soon as reasonably practicable –

- Correct the personal information if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully
- Destroy or delete the information if it is no longer authorised to retain that personal information
- Provide the data subject, to his or her satisfaction, with credible evidence in support of the information, or

- Where agreement cannot be reached between the responsible party and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the personal information in such a manner that it will always be read with the personal information, an indication that a correction of the personal information has been requested but has not been made

If the responsible party has taken steps that result in a change to the personal information and the changed personal information has an impact on decisions that have been or will be taken in respect of the data subject, the responsible party must, if reasonably practicable, inform each person or body to whom the personal information has been disclosed of the steps taken (i.e. to correct or destroy that personal information).

The responsible party must notify a data subject who has made a request in terms of section 24 of POPIA of the action taken as a result of the request.

13 PROCESSING SUBJECT TO PRIOR AUTHORISATION

Reference: Sections 57 and 58

Members should be aware that certain types of processing require the prior authorisation of the Information Regulator. The responsible party must obtain the prior authorisation of the Information Regulator before –

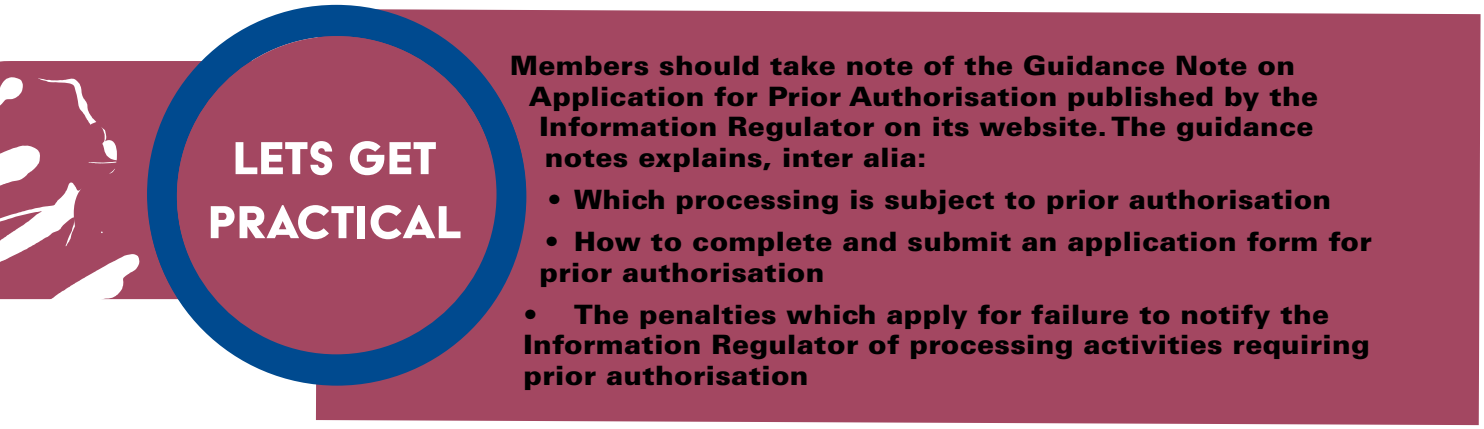
- Processing any unique identifiers of data subjects for a purpose other than the one for which the identifier was specifically intended at collection and with the aim of linking the information together with information processed by other responsible parties
- Processing information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties
- Processing information for the purposes of credit reporting, or
- Transferring special personal information or the personal information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information as referred to in section 72 of POPIA

Once the Information Regulator receives a notice that the responsible party wishes to perform processing activities which require prior authorisation, the Information Regulator must, within four weeks from the date of receipt of the notification, inform the responsible party whether or not the information officer will conduct a more detailed investigation.

Should the Information Regulator require a more detailed investigation, it must indicate the period within which it plans to conduct this investigation, which period must not exceed 13 weeks.

Once the Information Regulator has, in writing, authorised the processing of such personal information, then the responsible party proceeds with the processing activities.

A responsible party that has suspended its processing as required by section 58(2) and has not received the Information Regulator's decision within the time limit specified in sections 58(3) and 58(4) may presume a decision in its favour and continue with its processing.[9]



9 Note, however, that section 58(2) is now only effective from 1 February 2022.

14 DIRECT MARKETING BY UNSOLICITED ELECTRONIC COMMUNICATION

Reference: Section 69

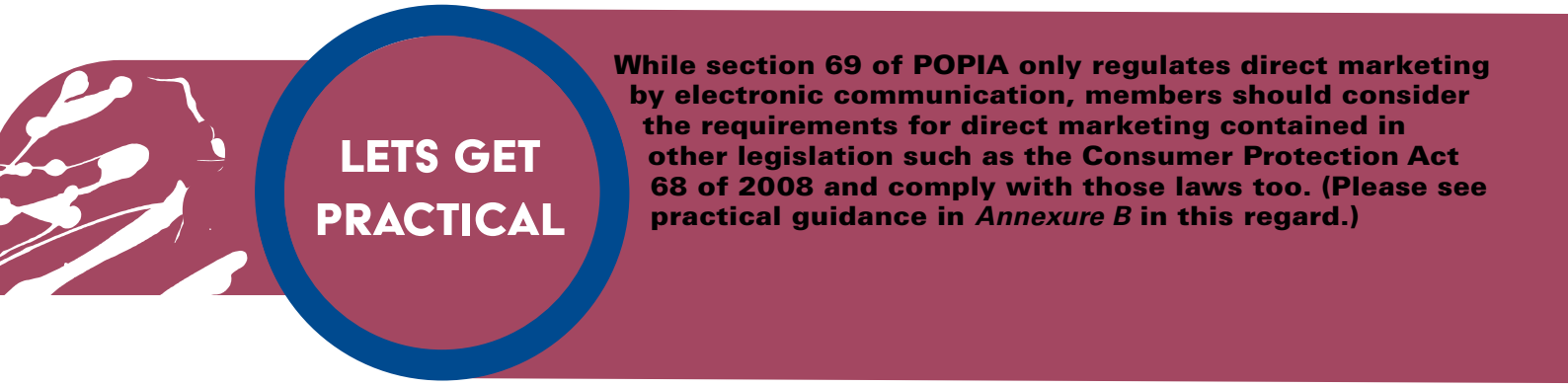
What is direct marketing?

'Direct marketing' is defined in POPIA as approaching a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of (a) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject, or (b) requesting the data subject to make a donation of any kind for any reason.

Type of direct marketing prohibited in terms of section 69 of POPIA

Although the definition of 'direct marketing' is wide and includes approaching a data subject either in person, by mail or by electronic communication, the prohibition in section 69(1) only applies to direct marketing via electronic communication.

Electronic communication means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient, and includes communications through automatic calling machines, facsimile machines, SMSs and emails



While section 69 of POPIA only regulates direct marketing by electronic communication, members should consider the requirements for direct marketing contained in other legislation such as the Consumer Protection Act 68 of 2008 and comply with those laws too. (Please see practical guidance in *Annexure B* in this regard.)

POPIA prohibits the processing of the personal information of the data subject for the purpose of direct marketing by means of any electronic communication unless the data subject (i.e. the recipient of the electronic communication) –

- Has given prior consent to his/her/its personal information being processed for direct marketing purposes, or
- Is a customer of a responsible party and the following conditions are satisfied:
  - The responsible party obtained the contact details of the customer in the context of a sale of a product or service
  - The responsible party will perform direct marketing only in respect of the responsible party's similar products and services, and
  - The responsible party has given the data subject a reasonable opportunity to object (free of charge and in a manner free of unnecessary formality) to the use of his electronic information both at the time when the information was collected and on the occasion of each communication with the data subject for the purpose of such direct marketing

Obtaining the data subject's consent for direct marketing

A responsible party may approach a data subject whose consent to direct marketing is required only once in order to request the data subject's consent to direct marketing. The responsible party may only approach the data subject for this purpose if the data subject has not previously withheld such consent.

Members must categorise information to be sent to clients in mandatory messages and optional messages. Clients must be provided the opportunity to ask to be removed from optional messages such as monthly newsletters and direct marketing communications.

If the member is targeting a new client, POPIA allows the member to contact the prospective client once to obtain consent to send direct marketing communications. If the prospective client does not answer, that is not viewed as consent and no unsolicited communication for direct marketing purposes must be sent.

Information to be included in direct marketing communications

Any communication for the purpose of direct marketing must contain –

- Details of the sender or the person on whose behalf communication is sent, and
- An address or other contact details for data subjects to opt out of the direct marketing

(For additional guidance on the topic of direct marketing please refer to *Annexure B*.)

15 AUTOMATED DECISION-MAKING

Reference: Section 71

A data subject may not be subject to a decision which results in legal consequences for him/her/it, or which affects him/her/it to a substantial degree, and which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person (including his/her performance at work, or his/her/its creditworthiness, reliability, location, health, and personal preferences or conduct).

The above prohibition does not apply if the decision –

- Is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects, or
- Has been taken in connection with the conclusion or execution of a contract, and –
  - – The request of the data subject in terms of the contract has been met, or
  - – Appropriate measures[10] have been taken to protect the data subject's legitimate interests

16 TRANS-BORDER INFORMATION FLOWS

Reference: Sections 57 to 59 and 72

A responsible party is prohibited from transferring personal information about a data subject to a third party who is in a foreign country unless:

- The third party who is the recipient of the information is subject to a law, binding corporate rules or a binding agreement which –
- Provides an adequate level of protection that is substantially similar to POPIA and effectively uphold the principles for reasonable processing of the personal information of data subjects that are natural persons and, where applicable, data subjects that are juristic entities, and
- Has provisions similar to POPIA relating to the further transfer of personal information from the recipient to third parties who are in a foreign country
- The data subject consents to the transfer
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject

10 These appropriate measures must –
- Provide an opportunity for a data subject to make representations about a decision made about him/her/it, and
- Require a responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information relating to him or her to enable him/her/it to make representations about the decision

- The transfer is necessary for the performance of a contract of between the data subject and the responsible party
- The transfer is necessary for the implementation of precontractual measures taken in response to the data subject's request, or
- The transfer is for the benefit of the data subject and it is not reasonably practicable to obtain the consent of the data subject to that transfer – but if it were reasonably practicable to obtain such consent, the data subject would be likely to give it

LETS GET PRACTICAL

Members should keep in mind that the Information Regulator's prior authorisation should be sought where the member intends on transferring special personal information or the personal information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information as contemplated above.

LETS GET PRACTICAL

The information officer must ensure that the responsible party's PAIA Manual and privacy notices include information regarding planned trans-border or cross border flows of personal information.

It should also be noted that once personal information has been transferred to the recipient in the foreign jurisdiction, the personal information will be subject to that country's data protection regulatory requirements when transferring the information to South Africa.

We suggest that you maintain a record of –

- **All foreign countries to which you are currently or planning to transfer personal information**
- **The manner in which you will legitimise the transfer of personal information to the recipient in the foreign jurisdiction (for example binding agreement / binding corporate rules, data subject consent, etc)**
- **If necessary, you may need to obtain a legal opinion regarding the adequacy of the foreign jurisdiction's law (only if you are not relying on another lawful justification for transferring personal information), and**
- **Prior authorisation obtained if such authorisation is mandated by POPIA**

17 WHAT TO DO IF YOU HAVE A DATA BREACH

Reference: Section 22

Reporting obligations

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person, the responsible party must notify the Information Regulator and the data subject unless the identity of the data subject cannot be established.

Timing

The responsible party must discharge its notification obligations as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Information Regulator determines that notification will impede a criminal investigation by the public body concerned.

Manner of notification

The notification to a data subject must be in writing and communicated in one of the following ways:

- Mailed to the last known physical address or postal address
- Sent by email to last known email address
- Placed on prominent position on the responsible party's website
- Published in news media, or
- As directed by the Information Regulator

The Information Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information if the Information Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

Content of notification

The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise and must include the following:

- A description of the possible consequences of the security compromise
- A description of the measures that the responsible party intends to take or has taken to address the security compromise
- A recommendation to the data subject with regard to the measures to be taken him/her/it to mitigate possible adverse effects of the security compromise, and
- If known, the identity of the unauthorised person who may have accessed or acquired the personal information

LETS GET PRACTICAL

Members should ensure that they have reasonable processes in place to detect and contain an information security breach (which includes, but is not limited to, a cyber incident). Members should implement formal plans regarding the manner in which a data breach will be handled.

18 REGULATORY BODIES' REQUEST FOR INFORMATION

In South Africa, various regulators often request information. These include public bodies such as the South African Revenue Service (SARS), the Companies and Intellectual Property Commission (CIPC) and the Financial Intelligence Centre.

There must always be lawful justification for processing personal information (including sharing personal information with external bodies). In this regard, POPIA states that personal information may be processed (for example shared) where processing complies with an obligation imposed by law on the responsible party.

Accordingly, where the law obliges the responsible party to provide regulators with certain information (including personal information) there will be a lawful basis to support that sharing provided that the responsible party does not share more personal information than is required in terms of law.

LETS GET PRACTICAL

For example, section 26 of the Tax Administration Act allows SARS to demand information from a third party (other than the taxpayer) for purposes of administration of a tax Act. The person receiving such a demand would be obliged to provide such information demanded in terms of the law, failing which it would be considered an offence.

Responsible parties should also consider the requirements of PAIA in terms of which it may be required or authorised to refuse to provide certain records of personal information to an external personal (including a regulator).

19 EXEMPTIONS UNDER POPIA

Exemption granted by the Information Regulator

Processing of personal information is not in breach of a condition for the processing of such information if the Information Regulator grants an exemption in terms of section 37 of POPIA.

In this regard, the Information Regulator may, by notice in the Government Gazette, grant an exemption to a responsible party to process personal information even if that processing is in breach of a condition for the processing of such personal information, or any measure that gives effect to such condition, if the Information Regulator is satisfied that, in the circumstances of the case –

- The public interest[11] in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing, or
- The processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing

In granting the exemption, the Regulator may impose reasonable conditions in respect of any exemption granted under subsection.

Exemptions that apply automatically

Processing of personal information is not in breach of a condition for the processing of such information if processing is in accordance with section 38 of POPIA. In this regard, personal information processed for the

11 The public interest includes –
- The interests of national security
- The prevention, detection and prosecution of offences
- Important economic and financial interests of a public body
- Fostering compliance with legal provisions established in the interests referred to under (b) and (c) above
- Historical, statistical or research activity, or
- The special importance of the interest in freedom of expression

purpose of discharging a relevant function[12] is exempt from certain sections of POPIA (set out in the table below) to the extent that compliance with such condition would be likely to prejudice the proper discharge of that function.

Sections which a responsible party may be exempt from in terms of section 38	Overview of the obligations of the section
Sections 11 (3) and (4) of POPIA	Allows the data subject to object to the processing of personal information in certain instances and requires the responsible party to cease processing following such an objection
Section 12 of POPIA	Requires the responsible party to collect of personal information directly from the data subject unless an exception in section 12(2) applies
Section 15 of POPIA	Prohibits the further processing of personal Information which is not in accordance with or otherwise incompatible with the original purpose of collection
Section 18 of POPIA	Requires the responsible party take reasonably practicable steps to ensure that the data subject is aware of the information contained in section 18 (i.e. informing the data subject of the responsible party's processing activities) unless an exception applies

LETS GET PRACTICAL

While the exemption in section 38 applies to public bodies, it can apply to members too where they are required in terms of law to report certain information to a regulatory authority to protect members of the public against –

- **Financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate, or**
- **Dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity**

20 FINES AND PENALTIES

POPIA creates a number of offences which can result in serious penalties for the responsible party. However, in this section we only consider the penalties that may be levied in circumstances that a responsible party has been found guilty of an offence in terms of POPIA. We also consider the Information Regulator's ability to levy administrative fines in certain circumstances.

Penal sanctions

Section 107 of POPIA provides that any person convicted of an offence in terms of POPIA is liable, in the case of a contravention of –

12 'Relevant function' means any function –
- Of a public body, or
- Conferred on any person in terms of the law which is performed with the view to protecting members of the public against –
  - Financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate, or
  - Dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity

- Section 100, 103 (1), 104 (2), 105 (1), 106 (1), (3) or (4) to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine and such imprisonment, or
- Section 59, 101, 102, 103 (2) or 104 (1) to a fine or to imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment

Despite anything to the contrary contained in any other law, a Magistrate's Court has jurisdiction to impose any penalty provided for in section 107 of POPIA.

Administrative fines

If a responsible party (the infringer) is alleged to have committed an offence in terms of POPIA, the Regulator may issue an infringement notice which may ultimately require the infringer to pay an administrative fine of up to R10 million.

ANNEXURE A – GLOSSARY

Data subject	The person to whom personal information relates
International guidelines	Any developing general international guidelines relevant to the better protection of individual privacy including guidelines published in terms of European data protection laws
Operator(s)	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
PAIA	Promotion of Access to Information Act 2 of 2000
Personal information	Information relating to an identifiable, living, natural person and, where applicable, an identifiable, existing juristic person, including, but not limited to – • Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, disability, religion, conscience, belief, culture, language and birth of the person • Information relating to the education or the medical, financial, criminal or employment history of the person • Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person • The biometric information of the person • The personal opinions, views or preferences of the person • Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence • The views or opinions of another individual about the person, and • The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person
POPIA	Protection of Personal Information Act 4 of 2013
Processing, processes and processed	Any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including – • The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use • Dissemination by means of transmission, distribution or making available in any other form. or • Merging, linking, as well as restriction, degradation, erasure or destruction of information
Responsible party	A public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information
SAICA	The South African Institute of Chartered Accountants
Special personal information	• 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, or • The criminal behaviour of a data subject to the extent that such information relates to – – The alleged commission by a data subject of any offence, or – Any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings

ANNEXURE B – DIRECT MARKETING GUIDANCE AND CHECKLIST

What is direct marketing?

Both the Protection of Personal Information Act 4 of 2013 (POPIA) and the Consumer Protection Act 68 of 2008 (CPA) define and regulate direct marketing. Both Acts define direct marketing as to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of

- Promoting or offering to supply, in the ordinary course of business, any goods and services to the data subject, or
- Requesting the data subject to make a donation of any kind for any reason

Do we need to consider and apply both POPIA and the CPA when performing direct marketing?

Section 2(9) of the CPA provides that if there are any inconsistency between any provision of the CPA and a provision of any other Act (such as POPIA) –

- The provisions of both Acts apply concurrently to the extent that it is possible to apply and comply with one of the inconsistent provisions without contravening the second, and
- To the extent where they cannot apply concurrently, the provision that extends the greater protection to a consumer prevails over the alternative provision

Similarly, section 3(2) of POPIA provides that POPIA applies to the exclusion of any provision of any other legislation that regulates the processing of personal information that is materially inconsistent with an object, or a specific provision of POPIA. However, if any other legislation provides for conditions for the lawful processing of personal information that are more extensive than those set out in Chapter 3 of POPIA, the extensive conditions prevail.

In a nutshell, those performing direct marketing must comply with both POPIA and the CPA and to the extent that there is any inconsistency must apply the Act with more stringent requirements.

Direct marketing in terms of POPIA

The prohibition against direct marketing in section 69 of POPIA only relates to direct marketing by means of any form of electronic communication.

Electronic communication is defined in POPIA as 'any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient'. Accordingly, direct marketing via electronic means includes, but is not limited, to communications sent via email, SMSs, automatic calling machines and fax. On the other hand, direct marketing via a telephone conversation, physical post or handing out flyers in person would not be regulated by section 69 of POPIA.

Direct marketing via electronic communication is prohibited unless the data subject (i.e. the recipient of direct marketing communication):

- Has given consent to the processing of his/her/its personal information for direct marketing purposes, or
- Is a customer of the responsible party and additional requirements (discussed below) have been satisfied

Direct marketing relying on consent

POPIA gives responsible parties the leeway to approach a data subject who has not previously withheld consent only once in order to request the consent of that data subject.

In order to perform direct marketing on the basis of consent, all the following requirements must be met:

- Consent must be voluntary (i.e. the data subject must have a genuine choice over whether or not to consent to direct marketing. Data subjects must not be coerced to provide consent or penalised for withholding consent)
- Consent must be specific (i.e. consent must be specific to processing for direct marketing activities by the responsible party and the type of communication preferred)

- Consent must be informed (i.e. the data subject should be provided with sufficient information to understand what they are consenting to)
- Consent must be an expression of will signifying agreement (i.e. consent should be a positive expression of choice – opt-in consent is preferred)
- The data subject's consent must be requested in a manner and form substantially similar to form 4 of the regulations (a copy of form 4 is available at the end of this annexure)

In addition to the above, it is recommended that the responsible party:

- Maintain a record of consent (this is a recommendation based on the fact that the responsible party bears the burden of proof that consent was granted in terms of section 11(2) of POPIA)
- Implement processes to remove data subjects from distribution lists once they have withdrawn consent and which ensure that direct marketing communications cease per the request of the data subject

Direct marketing to an existing customer

In order to perform direct marketing to existing customers who have not given their explicit consent, all the requirements below must be met:

- The responsible party has obtained the contact details of the data subject in the context of the sale of a product or service
- The responsible party may only process personal information for the purpose of performing direct marketing of the responsible party's own similar products or services
- The data subject has been given a reasonable opportunity to object, free of charge, to the use of his/her/its electronic details at the time when the information was collected, and
- The data subject has been given a reasonable opportunity to object, free of charge, to the use of his/her/its electronic details on the occasion of each communication with the data subject

Content of direct marketing communications

Once you have established that there is a lawful basis to send direct marketing to data subject(s), you must ensure direct marketing communications contain the minimum information prescribed by POPIA. In this regard the following requirements must be met in respect of each and every direct marketing communication:

- The communication contains details of the identity of the sender or the person on whose behalf the communication has been sent
- The communication contains an address or other contact details to which the recipient may send a request that such communications cease

Direct marketing in terms of the CPA

It is important to note that while POPIA restricts direct marketing via electronic means, section 11 of the CPA provides consumers the right to refuse to accept, require another person to discontinue, or to block any form of direct marketing (i.e. whether that direct marketing is conducted in person, by mail, by telephone or by electronic communication). Accordingly, in addition to complying with the requirements of POPIA as it pertains to direct marketing via electronic means, organisations need to comply with the requirements of the CPA as it pertains to direct marketing in the wider sense.

In this regard, section 11(2) of the CPA states that a person who has been approached for the purpose of direct marketing may demand during or within a reasonable time after that communication that the person responsible for initiating the communication desist from initiating any further communication (i.e. they may opt out at any time).

In giving effect to this right, section 11(4) of the CPA requires that any person authorising, directing or conducting any direct marketing must –

- Implement appropriate procedures to facilitate the receipt of demands that the direct marketing communication cease (i.e. implement a process that allows recipients of direct marketing to opt out of such communications)

- Not charge a consumer a fee for making a request that direct marketing communications cease
- Not perform direct marketing or allow another person to perform direct marketing to a person once a recipient has opted out
- Not perform direct marketing or allow another person to perform direct marketing to a person who has registered a relevant pre-emptive block against receiving direct marketing communications (i.e. registered on a recognised do not contact list once this list has been established/recognised by the National Consumer Commission)[13]

If a person has informed a direct marketer that he/she does not wish to receive direct marketing communication, the direct marketer should acknowledge the request in writing.

Timing of direct marketing communications

Section 12 of the CPA further regulates the dates and times that direct marketing can be sent to a consumer at his/her home. In this regard the following requirements should be adhered to:

A person must not engage in any direct marketing directed to a consumer at home for any promotional purpose during

- Sundays or public holidays contemplated in the Public Holidays Act 36 of 1994
- Saturdays before 09:00 and after 13:00, and
- All other days between the hours of 20:00 and 08:00 the following day

except to the extent that the consumer has expressly or implicitly requested or agreed otherwise.

Direct marketing may not be timed to be delivered to the consumer during the prohibited times referred to above unless expressly, in writing, agreed to by the consumer.

It should be noted that a direct marketer is not in breach of the above requirements if the communication was dispatched during the allowed period but only received by the consumer outside aforementioned period.

Additional recommendations as it pertains to direct marketing

- Give customers the option of selecting their preferred method of receiving direct marketing
- Always apply opt-in consent and do not pre-tick boxes for the data subject
- Perform small sample testing to assess the reliability of the data on your distribution lists
- Implement processes to deal with inaccurate information and data subject complaints related to direct marketing
- Disclose where you obtained the data subject's personal information and any other information that would be required from a transparency perspective especially where you are not relying on the explicit consent of the data subject to perform direct marketing
- Enter into agreements with external service providers who are conducting direct marketing on your behalf and agree on, inter alia, the manner in which –
  - The collection and withdrawal of consent will be managed
  - Data subject rights (including transparency requirements and requests related to the correction and deletion of personal information) will be handled and escalated
  - Complaints related to direct marketing activities will be handled and escalated

Do not sell or buy distribution lists unless there is clear evidence that the data subject has consented to the sharing of his/her/its details with third parties for purposes of those third parties performing direct marketing.

Ensure that opting out is as easy as opting in (for example by including an opt-out by an unsubscribe link or by sending a message).

Do not send direct marketing from a hidden number / private number.

13 Note that section 11(3) of the CPA allows the National Consumer Commission to establish or recognise a registry in which any person may register a pre-emptive block, either generally or for specific purposes, against any communication that is primarily for the purpose of direct marketing. As at the date of issuing this version of the SAICA Guide, the National Consumer Commission has not established or authoritatively recognised such a registry.

Form 4 – Regulations relating to the Protection of Personal Information (GNR 1383 of 14 December 2018: Government Gazette 42110)

FORM 4

APPLICATION FOR THE CONSENT OF A DATA SUBJECT FOR THE PROCESSING OF PERSONAL INFORMATION FOR THE PURPOSE OF DIRECT MARKETING IN TERMS OF SECTION 69 (2) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 6.]

TO:

(*Name of data subject*)

FROM:

Contact number(s):

Fax number:

E-mail address:

(*Name, address and contact details of responsible party*)

Full names and designation of person signing on behalf of responsible party:

Signature of designated person

Date:

PART B

I, (*full names of data subject*) hereby:

	Give my consent.

To receive direct marketing of goods or services to be marketed by means of electronic communication.

SPECIFY GOODS or SERVICES:

SPECIFY METHOD OF COMMUNICATION:

FAX:

E - MAIL:

SMS:

OTHERS - SPECIFY:

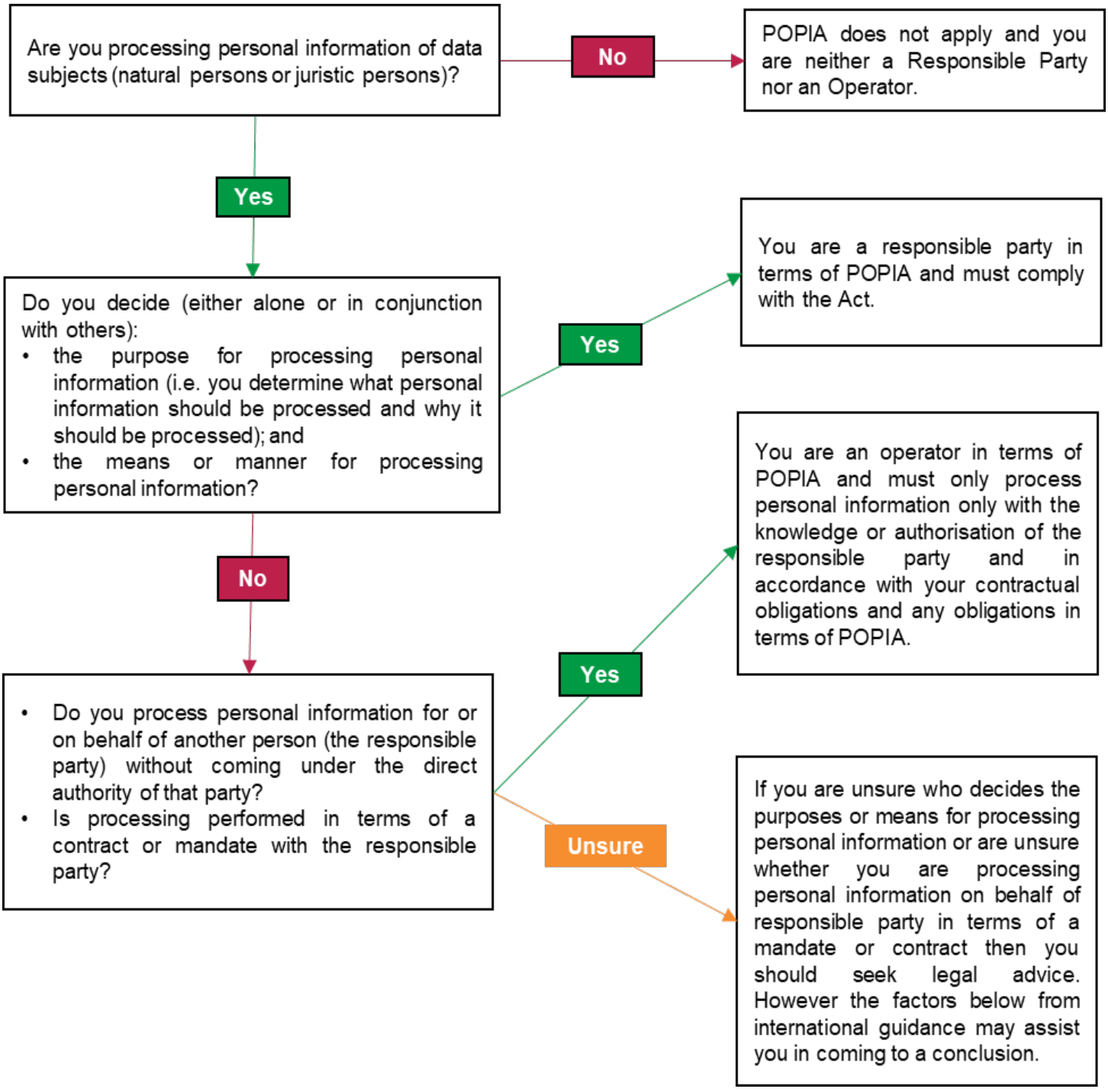
Signed at this day of 20

Signature of data subject

ANNEXURE C – RESPONSIBLE PARTY VERSUS OPERATOR

Decision tree

All private and public bodies should analyse their processing activities and determine in what capacity they have collected and are processing that personal information (ie as a responsible party or as an operator). Whether you are acting in the capacity of a responsible party or operator will depend on the specific circumstances of the processing activity. It is possible to be a responsible party for some processing activities and an operator for other processing activities. The decision tree below intends to provide some guidance to organisations, but it is recommended that you seek specialist legal advice where you are uncertain regarding the capacity in which you process personal information.



Additional factors to consider

The below factors may assist you determining whether you are a responsible party or an operator in terms of POPIA. These factors originate from guidelines published by the European Data Protection Board on the concepts of 'controller' and 'processor' in the GDPR and the Guide to the GDPR published by the UK's Information Commissioner's Office, but have been adapted for the South African context. It is important for members to keep abreast of local guidance which may be published by the Information Regulator in due course to determine the capacity in which personal information is being processed.

FACTORS INDICATING THAT YOU ARE A RESPONSIBLE PARTY
• You obtain a commercial or other benefit from, or have an interest in, the processing (other than the renumeration for services paid by another responsible party) • You make decisions about the data subjects concerned as part of or as a result of the processing • You exercise professional judgement in the processing of the personal information • The processing activities can be considered as naturally attached to the role or activities of your organisation (for example due to traditional roles or professional expertise) which entails responsibilities from a data protection point of view • The processing refers to your relationship with the data subjects as employees, customers, members, etc • You are processing the personal information as a result of a contract between yourself and the data subject • You have entrusted the processing of personal information to an external organisation to process the personal information on your behalf (i.e. an operator) • You have complete autonomy in deciding how the personal information is processed • You decided – – To collect or process the personal information – What the purpose or outcome of the processing was to be – Which personal information should be collected – About which individuals to collect personal information – You and (an)other party(ies) are involved jointly determine the purposes and means of the processing. You and another party/parties have a decisive influence over whether and how the processing takes place – either by a common decision or by converging decisions that complement each other and are necessary for the processing because they have a tangible impact on the determination of the purposes and means • Where the professional service provider is engaged by their clients based on general instructions to perform professional services (for example to complete the client's tax return or to perform accounting services) • Where the professional service provider processes personal information in accordance with its statutory obligations (for example when an auditor is reporting client information in accordance with a statutory reporting obligation) • Where the professional services provider is processing personal information in accordance with its professional rules or codes of conduct (for example when an auditor performs an audit in accordance with professional rules)

FACTORS THAT INDICATE YOU ARE AN OPERATOR

- You process the personal information for another party's purposes and in accordance with its documented instructions – you do not have a purpose of your own for the processing
- Another party monitors your processing activities to ensure that you comply with instructions and terms of contract
- You do not pursue your own purpose in the processing other than your own business interest to provide services
- You have been engaged for carrying out specific processing activities by someone who in turn has been engaged to process data on another party's behalf and on this party's documented instructions
- You do not decide –
  - To collect personal information from individuals
  - What personal information should be collected from individuals
  - The lawful basis for the use of that personal information
  - What purpose or purposes the personal information will be used for
  - Whether to disclose the data, or to whom
  - How long to retain the personal information
- You may make some decisions on how personal information is processed but implement these decisions under a contract with someone else
- You are not interested in the end result of the processing
- Where a professional services provider is processing personal information where the client has given detailed instructions on the personal information to be processed, the purpose for processing such personal information and the means for processing such personal information (for example performing agreed-upon procedures if the client has given detailed instructions)

ANNEXURE D1 – PRIVACY TOPICS TO BE CONSIDERED IN ENGAGEMENT LETTERS WITH CLIENTS

Obligations of the member

Include here those obligations that pertain specifically to the member where it processes personal information in the capacity of a Responsible Party, such as the responsibility to ensure lawful processing of personal information.

Alternatively, where member is acting in the capacity of an operator, and where the client is the Responsible Party, include an obligation for the member to process personal information only in terms of the instructions and mandate of the client.

Information required to perform services

Explanation that personal information may need to be processed to perform the services of the member.

Oblige the client to provide the member with access to information (including personal information) in the client's possession or control that is needed by the member in providing its services to the client.

Also record the member's responsibilities when collecting personal information from sources other than the client.

Description of agreed security safeguards

The member's obligations to implement appropriate and reasonable technical and organizational measures to:

- regularly identify all reasonably foreseeable internal and external risks to personal information in their possession or under their control;
- to establish and maintain appropriate safeguards against the risks identified;
- to regularly verify that the safeguards are effectively implemented; and
- to ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards should be recorded.

The minimum security safeguards that are agreed between the member and the client should be specified for example in an Annexure.

Subcontracting of processing to a third party

This section should govern whether or not the member may subcontract any of its services, entailing the processing of the client's personal information, to another person.

This section should also include any additional requirements or conditions that the member must comply with in order to subcontract processing of client's personal information to a third party, including:

- requiring the member to enter into a written subcontracting agreement with the third party which imposes, in substance, the same obligations on the third party as are imposed on the member in respect to the processing of personal information;
- whether prior written consent of the client would need to be met before entering into such subcontracting arrangement).

International transfers

This section should record whether any international transfer of personal information (i.e. transferring personal information to any jurisdiction outside of South Africa) will occur. The agreement should also record any specific conditions which are agreed between the member and the client in respect of the international transfer of personal information.

Confidentiality

In this section the member may record that the employees providing services will be required to enter into a confidentiality undertaking.

Reporting requirements

In this section record that there may be an obligation to report personal information to external regulators or external bodies in accordance with a statutory requirement or professional obligation.

The member may wish to specify the circumstances when this would apply for example in the case of reportable irregularities or where these is non-compliance with laws and regulations (e.g. NOCLAR).

Sharing of personal information

This section should include any anticipated sharing of personal information for example intragroup transfers, to the extent applicable.

Use of personal information

This section should detail any additional use of personal information for example provide a block to indicate whether or not the client consents to the use of its personal information for direct marketing purposes or to allow the member to use client personal information for credential purposes.

Notification and assistance to be provided by the member and client

This section should detail the member's obligations to notify the client of certain instances arising, which may include such things as :

- any legally binding request for disclosure of the personal information by a law enforcement authority (unless the either party is legally prohibited from notifying the other);
- any accidental or unauthorised loss of, damage to or destruction of personal information;
- any unauthorised processing of personal information.

It is recommended that the manner in which this notification must be provided is specified and the relevant contact details of the parties are included in an Annexure which can be updated from time to time.

Obligations in the case of a personal information breach

This section should detail the member's obligations to notify the client of suspected personal information breaches where the member has reasonable grounds to believe that the personal information records made accessible by the client has been accessed or acquired by any unauthorised person.

It is recommended that the manner in which this notification must be provided is specified and the relevant contact details of the parties are included in an Annexure which can be updated from time to time.

Obligation after the termination of personal information processing services

This section should detail the manner in which personal information records should be handled on the termination of the agreement. For example, the agreement could require that the client should elect whether personal information records (including any copies made) should be returned to the client or destroyed by the member.

This section should also make provision for the member retaining any records it is authorised to retain in terms of POPIA, any professional rules and/or any particular laws.

Breach and indemnification

In this section the consequences for non-compliance with the requirements of the agreement should be made clear.

ANNEXURE D2 – TOPICS TO BE CONSIDERED IN ENGAGEMENT LETTERS WITH OPERATORS

Description of processing and mandate of the operator

The processing activities, and in particular the categories of personal information processed and the purposes for which the personal information is processed, by the operator on behalf of the responsible party.

Obligations of the responsible party

Those obligations that pertain specifically to the responsible party such as the responsibility to ensure lawful processing of personal information and to obtain the prior authorisation of the Information Regulator, where applicable.

Operator's obligation to process personal information in accordance with mandate

In this section include clause which obliges the operator to:

- Process personal information only for the specific, explicit and legitimate purposes of processing specified by the responsible party. It is recommended that the categories of personal information, categories of data subject and the purposes of processing be recorded in a separate annexure
- Process personal information only with the knowledge and written authorisation of the responsible party unless processing is required by law or in the course of the proper performance of its duties
- Treat personal information which comes to its knowledge through the provision of services to the responsible party as confidential and to not disclose it unless required by law or in the course of the proper performance of its duties
- Inform the responsible party of any legal requirement obliging the operator to process personal information contrary to the responsible party's written authorisation before conducting such processing, unless that law prohibits the operator from informing the responsible party of such processing
- Process personal information in accordance with the terms of this agreement and to inform the responsible party if it is unable comply with the terms of the agreement. Also include consequences where the operator is unable to comply with the agreement (examples may include the suspension of processing or the termination of broader agreements)

Operator to implement reasonable and appropriate security safeguards

In this section the operator agrees and warrants that it has implemented reasonable technical and organisational measures to regularly identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control; to establish and maintain appropriate safeguards against the risks identified; to regularly verify that the safeguards are effectively implemented; and to ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

The minimum security safeguards that the responsible party considered reasonable and adequate for the operator to implement should be specified for example in an annexure.

Operator to demonstrate compliance (privacy audits)

In this section the operator should be obliged to make available all information necessary to demonstrate compliance with POPIA and the terms of this agreement to the responsible party (for example copies of audit reports in respect of its POPIA control environment).

This section should also allow the responsible party to perform audits of the operator's systems, facilities, and controls to measure compliance against the requirements of POPIA and/or compliance of the agreement between the parties. The agreement should specify whether the responsible party and/or an external third party may conduct such an audit.

Outsourcing of processing to a third party

This section should govern whether or not the operator may subcontract any of its processing operations performed on behalf of the responsible party and whether i.the prior written consent of the responsible party

would be needed in this regard.

This section should also include any additional requirements that the operator must comply with in order to outsource processing to a third party (for example requiring that the operator must enter into a written agreement with the third party which imposes, in substance, the same obligations on the third party as are imposed on the operator).

International transfers

This section should generally prohibit the operator from transferring personal information to any jurisdiction outside of South Africa without the prior written consent of the responsible party.

Notification and assistance to be provided by the operator

This section should detail the operator's obligations to notify the responsible party of certain instances arising, which may include:

- Any legally binding request for disclosure of the personal information by a law enforcement authority (unless the operator is legally prohibited from notifying the responsible party)
- Any accidental or unauthorised loss of, damage to or destruction of personal information
- Any unauthorised processing of personal information
- Where the operator has become aware that the personal information being processed by it is inaccurate, misleading or has become outdated

It is recommended that the manner in which this notification must be provided be specified and the relevant contact details of the parties be included in an annexure which can be updated from time to time.

Obligations in the case of a personal information breach

This section should detail the operator's obligations where it has reasonable grounds to believe that the personal information of one or more data subject(s) has been accessed or acquired by any unauthorised person. Such obligations should include the operator's obligation to notify the responsible party without undue delay of the breach / suspected breach and furnish the responsible party with the information set out in section 22 of POPIA to the extent that this information is available or becomes available.

It is recommended that the manner in which this notification must be provided be specified and the relevant contact details of the parties be included in an annexure which can be updated from time to time.

Obligation after the termination of personal information processing services

This section should detail the manner in which personal information records should be handled on the termination of the agreement generally the responsible party should elect whether personal information records (including any copies made) should be returned to the responsible party or destroyed by the operator. This section should also make provision for the operator providing certain assurances that personal information has been destroyed.

Assistance with data subject participation rights, complaints and investigations

This section should oblige the operator to promptly refer any request or demand received directly from the data subject in relation to his/her/its personal information and any complaints in terms of POPIA to the responsible party.

The operator should be obliged to assist the responsible party in handling requests or complaints. However, the extent of assistance should be determined by the responsible party having regard to the nature of the operator's processing activities and its relationship with data subjects.

This section should also oblige the operator to co-operate and support the responsible party where the responsible party's processing activities are under investigation (for example by providing relevant information to the responsible party / Information Regulator).

Breach and indemnification

In this section the consequences for non-compliance with the requirements of the agreement should be made clear. The responsible party may also want to seek indemnification against financial loss caused by the operator's failure to comply with the terms of the agreement.

ANNEXURE E – LAWFUL BASIS FOR PROCESSING PERSONAL INFORMATION CHECKLIST

Personal information cannot be processed unless there is at least one lawful justification which allows the processing of personal information as contemplated in section 11(1) of POPIA. Different lawful justifications will likely apply to the different processing activities of a responsible party. There may also be more than one lawful justification that may be relied on, but there must always be at least one justification that applies.

It is recommended that you record the lawful justification for processing personal information per processing activity for example in a personal information inventory or other document to evidence compliance with POPIA.

Yes/No	Lawful justification in terms of section 11 of POPIA	Explanation
	Has the data subject consented to the processing of personal information?	POPIA is not specific regarding the mechanism for managing consent. However, for consent to be valid, it must – • Be voluntary (i.e.i.e. it cannot be coerced or forced and the data subject must have a genuine choice) • Be specific (i.e. blanket consent to all processing is not recommended) • Be informed (i.e. the responsible party must be transparent and provide the data subject with all relevant information required to make an informed decision) • Be a clear expression of will in terms of which permission is given to the processing activities Section 11(2)(a) provides that the responsible party bear the burden of proof for the data subject's or competent person's consent. When obtaining consent, it is advisable for the responsible party to keep proof of consent (for example by obtaining written consent in a consent form or keeping a record of electronic consent given in a repository, or keeping a voice recording in a central repository). It must be borne in mind that consent can be withdrawn by the data subject at any time. Accordingly, the responsible party must implement mechanisms to manage consent so that when a data subject withdraws consent his/her/its personal information is no longer processed by the responsible party.
	Be voluntary (i.e.i.e. it cannot be coerced or forced and the data subject must have a genuine choice)	
	Is the processing of personal information necessary to carry out the actions for the conclusion or performance of a contract that the data subject is a party to? (I.e. have you concluded a contract with a data subject that requires his/her/its personal information to be processed in order to conclude the contract or to perform in terms of the contract?)	It is important to determine whether or not the personal information being collected for the purpose of conclusion or performance of a contract with a data subject is necessary and not excessive. A contract should not require the provision of unnecessary information that is not linked to the purpose of collection. You can rely on this lawful justification if you need to process personal information – • To deliver a contractual service or to perform a contractual obligation, or • Where the data subject has asked you to do something (for example provide a quotation) which will inform the data subject of whether or not he/she/it wants to enter into a contract

	Does processing of personal information comply with an obligation imposed by law on the responsible party? (I.e. is there a law that requires you to process personal information?)	This lawful justification applies if you are obliged to process personal information to comply with a common law or statutory obligation. You should document the specific statutory provision or common law obligation that requires the processing of personal information. For example, when auditors review annual financial statements, the Companies Act requires them to verify accuracy by checking bank statements, share certificates, CIPC director information, and tax and VAT returns in order to satisfy the relevant reporting standards. Processing of the aforementioned documents is therefore imposed by legislation.
	Are you a public body and, if so, is the processing of personal information necessary for the proper performance of a public law duty by you?	This lawful justification may only be relied upon by public bodies and to the extent that processing is necessary for the proper performance of a public law duty. For example, SARS has powers to collect personal information in accordance with tax legislation and for the proper performance of their statutory obligations. Note that data subjects have a right to object to processing on reasonable grounds relating to the data subject's particular situation (unless legislation provides for such processing) where this lawful basis is relied on.
	Does the processing of personal information protect a legitimate interest of the data subject?	Note that data subjects have a right to object to processing on reasonable grounds relating to the data subject's particular situation (unless legislation provides for such processing) where this lawful basis is relied on. For example, there is a strong argument that sharing relevant personal information of an employee to paramedics in the case of a medical emergency (such as medical aid information or known allergies) protects a legitimate interest of the data subject.
	Is the processing of personal information necessary for pursuing the legitimate interests of the responsible party?	At date of publishing hereof, the Information Regulator has not issued guidance regarding when it would be appropriate to rely on this lawful basis for processing personal information. Based on guidelines from international guidance, in particular the ICO's Guide to the GDPR, when relying on this justification responsible parties should note: • Based on international guidance published by the ICO and former Working Party 29 in Europe, legitimate interests may include for example: – Enforcement of legal claims including debt collection via out-of-court procedures – Prevention of fraud, misuse of services, or money laundering – Employee monitoring for safety or management purposes – Whistle-blowing schemes – Physical security, IT and network security

	Is the processing of personal information necessary for pursuing the legitimate interests of a third party to whom the information is supplied?	• While 'legitimate interests' can be interpreted to encompass a range of interests, responsible parties should not assume it will always be acceptable to rely on this justification and will need to motivate:
		  • That there is a legitimate interest (you should describe and articulate what that legitimate interest is)
		  • That the processing is necessary in pursuing the said legitimate interest (i.e. the processing you wish to do must be sufficiently linked to pursuing the legitimate interest)
		  • The data subject's rights to privacy have not been unjustifiably compromised for the sake of achieving the legitimate interest (for example there is no reasonable less intrusive mechanism for achieving the legitimate interest)
		• It is recommended that you not rely on vague or generic business interests but rather specify exactly what legitimate interest you are trying to achieve and why the processing activity is required to achieve it. You should also motivate why the legitimate interest outweighs the data subject's rights to privacy and that there is no reasonable, less intrusive mechanism for pursuing these interests. You should keep a record of this analysis to evidence that you have reasonably applied your mind to the applicability of the justification to the processing activities.
		• Some of the questions you should consider based on guidance from the ICO are:
		  – Why do you want to process the personal information?
		  – Who benefits from the processing and how?
		  – What would the impact be if you couldn't go ahead with the processing?
		  – Would your use of the personal information be unethical or unlawful in any way?
		  – Does this processing actually help to further the identified legitimate interest?
		  – Is the processing reasonable or is there another less intrusive way to achieve the same result?
		  – What is the nature of your relationship with the data subject?
		  – Is any of the personal information particularly sensitive?
		  – Would data subjects expect you to use their data in this way and are you happy to explain it to them?
		  – Are some data subjects likely to object or find it intrusive?
		  – What is the possible impact on the data subject and how serious is the impact?
		  – Are you processing children's personal information or the personal information of more vulnerable sectors of society?
		  – Can you adopt any safeguards to minimise the impact?
		  – Can you offer an opt-out to data subjects?
		• You should ensure that data subjects are made aware of your reliance on this justification to process their personal information and inform them of their right to object to processing on reasonable grounds relating to the data subject's particular situation (unless legislation provides for such processing)

ANNEXURE F – BASIC INFORMATION SECURITY CHECKLIST FOR SMALL, LOW-RISK BUSINESS OWNERS

- This basic information security checklist has been developed to assist small, low-risk business owners with POPIA compliance. The list is not exhaustive and each organisation's risk profile and exposure may vary. Organisations are encouraged to conduct a periodic risk assessment to determine whether a change in the risk profile requires additional safeguards to be implemented. Generally accepted information security standards and guidelines can be consulted for additional information.
- Do you have a register (that records the information owner, storage locations and description) to record physical and electronic information assets? Information protection starts with a good understanding of the assets that are under the organisation's control, where personal information is accessed, shared and stored.
- Are the roles and responsibilities with regard to information security defined and clearly communicated in the organisational policies and employment contracts? The responsibility and accountability for information security is a shared amongst all stakeholders in the organisation.
- Do you continually educate your staff on the information security risks related to personal information protection? The human element of information security is often targeted by threat actors and is seen as one of the weakest links in the security chain. Regular security awareness sessions can be used to reinforce secure behaviour amongst staff members.
- Do you have adequate physical security to protect your organisation's premises? Do you limit access to rooms and cabinets where physical records containing personal information are stored? How are your data centres physically secured (such as lock and key, biometric access, key card)? Personal information breaches are not limited to the electronic world, and physical loss or theft remains a risk.
- Do you protect mobile devices containing personal information, including smartphones, tablets and laptops? Also consider that employee personal devices ('Bring your own device' or BYOD) are often used to access personal and other sensitive information.
- Do your contracts with data operators (or key technology services providers) include the appropriate privacy clauses and require these third parties to implement information security controls to protect your assets?
- Do you delete personal information after it is no longer necessary for the purpose of collection, and do you securely dispose of IT assets to ensure that personal information cannot be retrieved? Information stored on discarded data storage equipment (such as hard drives) that are not adequately cleared can often be recovered in a readable format using specialised software and equipment.
- Have you adequately backed up your business-critical information and does the process include at least one copy stored off site (not at the same premises as the live data) and offline (not network connected, for example on a backup tape)? The ability to recover backed up information within an acceptable timeframe is an important consideration and should be periodically tested.
- Do you have logical access controls, including strong passwords and multifactor authentication (MFA) to secure applications and services that store and process personal information? Passwords are often compromised during malicious privacy breaches and multifactor authentication is a proven mitigating factor.
- Have you secured your remote and cloud-based applications, including productivity and collaboration tools? Working from home has increased the potential for information security breaches. The responsibility to secure personal information stored and processed on cloud services remain with the responsible party.
- Have you implemented a securely configured firewall to protect your network from attacks originating from the internet? A firewall can be an effective network defence control and should be reviewed to ensure that the device has been appropriately configured.
- Have you securely configured your organisation's wi-fi network? Secure protocols and complex passwords can be used to mitigate the threat of data interception over wireless networks.
- Have you implemented an anti-virus solution to identify and prevent malware from spreading on your network? Anti-malware can be effective in preventing malicious software on IT systems and should be consistently installed and updated.
- Have you secured your email solution to identify and prevent malicious email (including phishing, malware, fraud, etc) and block it from reaching your organisation's mailboxes? Preventing malicious email from reaching your staff mailboxes is an effective way to reduce threats.

- Do you regularly install patches and security updates on your IT systems including network infrastructure, mobile devices, operating systems and applications? Security incidents often occur as a result of outdated and vulnerable software platforms. Vulnerability assessments can be used to identify these issues and recommend solutions to address them.
- Do you use encryption technologies to protect the confidentiality of personal information on the systems and databases where it is stored, as well as in transmission? While encryption may not be able to prevent an information breach, it can protect the confidentiality of the information and the affected data subjects.
- Have you established an incident response process supported by a documented plan to effectively manage a privacy information breach (or other security incidents) in line with POPIA requirements? Despite implementing preventative measures, privacy incidents may still occur. An effective privacy incident response plan can help to minimise the impact while ensuring that your organisation conforms to POPIA regulations.

ANNEXURE G – TEMPLATE TO DOCUMENT FINDINGS OF PERSONAL INFORMATION IMPACT ASSESSMENT

Regulation 4 of the POPIA Regulations makes it the information officer's responsibility to ensure that a personal information impact assessment is done to ensure that adequate measures and standards are in place in order to comply with the conditions for the lawful processing of personal information in terms of POPIA. At the time of publishing this guide, the Information Regulator has not published guidance regarding the manner in which a privacy impact assessment must be performed. Accordingly, information officers are encouraged to engage with privacy specialists and the Information Regulator and to consider the practices in leading privacy jurisdictions in determining how to perform a personal information impact assessment. This document aims to assist you in documenting the results of your assessment and provides examples of the types of information you may want to consider in conducting the privacy impact assessment. However, you should adapt this template as you consider necessary to fulfil your obligations under POPIA. It is recommended that you formally document the personal information impact assessment process to be followed by the organisation (including the formal approval process).

PERSONAL INFORMATION IMPACT ASSESSMENT REPORT

Responsible party:	
Project name / processing activity:	
Date of assessment:	
Information officer:	
Overall risk rating of report (high, medium, low):	

PART A: CONTEXT

1. Overview of processing/project

[Describe the project / processing activities and the context of the project / processing activities. Include a description of the purpose of the project / processing activities, whether the project/processing is a long-term activity or once-off activity, and explain at what point of the project / processing activity this assessment is being performed.]

2 Scope and approach of assessment

[Describe the scope of the assessment (i.e. what systems, processes, business units, etc) were considered and what the limitations of the assessment are. Describe how the assessment was performed (for example what information was considered, who was interviewed or consulted, whether external advice was sought, etc).]

PART B: RISKS RELATED TO TYPES OF PERSONAL INFORMATION BEING PROCESSED

OVERALL RISK RATING FOR PART B:	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

1 Data subjects and personal information

<u>Categories of data subjects and personal information</u>

- Describe the categories of data subjects impacted by the project / processing activities. Document whether the data subjects are children or otherwise considered more vulnerable sectors of society. consider whether the data subjects are likely to be literate. Consider whether the data subject has access to internet and website services of the responsible party.]
- [Describe categories of personal information involved (if applicable, also record all new personal information involved as a result of the project). Document whether there more sensitive categories of personal information will be processed, such as special personal information or account numbers.]

Privacy risks and considerations

[Describe at a high level any privacy risks or special considerations that should be considered in more detail with regard to the categories of data subjects and/or the categories of personal information involved.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

2 Processing of special personal information (sections 26 to 33)

Summary of POPIA requirement

A responsible party may not process special personal information unless:

- A general exception in section 27(1)[14] of POPIA applies
- The Regulator may, upon application by a responsible party and by notice in the Government Gazette, authorise a responsible party to process special personal information on the basis that such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the data subject
- An exception in section 28 applies and the requirements of that section are complied with insofar as the processing of a data subject's religious or philosophical beliefs is concerned
- An exception in section 29 applies insofar as the processing of a data subject's race or ethnic origin is concerned
- An exception in section 30 applies and the requirements of that section are complied with insofar as the processing of a data subject's trade union membership is concerned
- An exception in section 31 applies and the requirements of that section are complied with insofar as the processing of a data subject's political persuasion is concerned
- An exception in section 32 applies and the requirements of that section are complied with insofar as the processing of a data subject's health or sex life is concerned
- An exception in section 33 applies and the requirements of that section are complied with insofar as the processing of a data subject's criminal behaviour or biometric information is concerned

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity / project having regard to requirements above. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

14 The exceptions in section 27(1) are:
- Processing is carried out with the consent of a data subject referred to in section 26
- Processing is necessary for the establishment, exercise or defence of a right or obligation in law
- Processing is necessary to comply with an obligation of international public law
- Processing is for historical, statistical or research purposes to the extent that –
  - The purpose serves a public interest and the processing is necessary for the purpose concerned, or
  - It appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the Processing does not adversely affect the individual privacy of the data subject to a disproportionate extent
- Information has deliberately been made public by the data subject, or
- The provisions of sections 28 to 33, as the case may be, are complied with

3 Processing of a child's/children's personal information (sections 34 to 35)

Summary of POPIA requirement

A responsible party may not process the personal information of a child/children unless an exception in section 35 applies and the requirements of that section are complied with.

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity / project having regard to requirements above. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

4 Processing of account numbers (section 105)

Summary of POPIA requirement

A responsible party who contravenes the provisions of condition 1 of POPIA insofar as those provisions relate to the processing of an account number[15] of a data subject is guilty of an offence.

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity/project having regard to requirements above. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

PART C: RISKS RELATING TO THE TRANSFER OF PERSONAL INFORMATION

OVERALL RISK RATING FOR PART C	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

15 'Account number' means any unique identifier that has been assigned to one data subject only, or jointly to more than one data subject, by a financial or other institution which enables the data subject to access his, her or its own funds or to access credit facilities or which enables a data subject to access joint funds or to access joint credit facilities (as the case may be).

1 Personal information flows

Data flows/access

[Document the current flow of personal information (and, if applicable, the future flow of personal information to the extent that the project will cause a change). Name the external parties that will have access to the personal information of data subjects and determine whether there is any international transfer of personal information. Document the places, departments or systems where personal information will be transferred.]

Privacy risks and considerations

[Describe at a high level any privacy risks or special considerations that should be considered in more detail with regard to the data flows involved.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

2 International transfers (section 72)

Summary of POPIA requirement

A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless –

- The third party who is the recipient of the information is subject to a law, binding corporate rules[16] or binding agreement which provide an adequate level of protection that –
  - Effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person, and
  - Includes provisions that are substantially similar to this section relating to the further transfer of personal information from the recipient to third parties who are in a foreign country
- The data subject consents to the transfer
- The transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party, or
- The transfer is for the benefit of the data subject and –
  - It is not reasonably practicable to obtain the consent of the data subject to that transfer, and
  - If it were reasonably practicable to obtain such consent, the data subject would be likely to give it

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity / project having regard to requirements above. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

16 Section 72(2) defines 'binding corporate rules' to mean personal information processing policies, within a group of undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country, and 'group of undertakings' to mean a controlling undertaking and its controlled undertakings.

PART D: ASSESSMENT OF RISKS AND COMPLIANCE WITH THE EIGHT CONDITIONS OF POPIA

OVERALL RISK RATING FOR PART D	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

1 Condition 1 – Accountability

(section 8)

Summary of POPIA requirement

The responsible party must ensure that the conditions set out in POPIA, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity/project. Also consider whether there are any specific codes of conduct which needs to be complied with that are applicable to the responsible party. Describe any areas of current non-compliance with the requirements / codes of conduct.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

2 Condition 2 – Processing limitation

Lawfulness of processing (section 9)

Summary of POPIA requirement

Personal information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity/project having regard to the above requirement. Consider whether the processing is reasonable with regard to the rights of data subjects to privacy. Consider whether processing may be considered unlawful. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above. Consider whether the purpose for processing can reasonably be achieved in a less intrusive manner.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

3 Condition 2 – Processing limitation

Minimality (section 10)

Summary of POPIA requirement

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

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity/project. For example, consider whether personal information being collected and processed is irrelevant, inadequate or excessive with regard to the purpose for which it is intended to be processed. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

4 Condition 2 – Processing limitation

Lawful justification (section 11)

Summary of POPIA requirement

Personal information must be processed if there is a lawful basis or justification in terms of section 11(1)[17]. Where consent is relied upon, the responsible party must be able to evidence consent and must implement processes which give effect to a data subject's withdrawal of consent to ensure that the processing ceases. When relying on a justification in section 11(1)(d) to (f), processes must be in place to handle objections by the data subjects.

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity/project with regard to the requirements above. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

17 Section 11(1) sets out the following justifications for processing personal information:
- The data subject, or a competent person where the data subject is a child, consents to the processing
- Processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party
- Processing complies with an obligation imposed by law on the responsible party
- Processing protects a legitimate interest of the data subject
- Processing is necessary for the proper performance of a public law duty by a public body, or
- Processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied

5 Condition 2 - Processing limitation

Collection directly from the data subject (section 12)

Summary of POPIA requirement

Personal information must be collected directly from the data subject unless an exception in section 12(2)[18] of POPIA applies.

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity/project with regard to the requirements above. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

6 Condition 3 - Purpose specification

Collection for a specific purpose (section 13)

Summary of POPIA requirement

- Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.
- Furthermore, steps must be taken (in accordance with section 18(1) of POPIA) to ensure that the data subject is aware of the purpose of collection, unless an exception in section 18(4) of POPIA applies.

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity / project having regard to requirements above. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

18 The exceptions in section 12(2) of POPIA are:
- The information is contained in or derived from a public record or has deliberately been made public by the data subject
- The data subject, or a competent person where the data subject is a child, has consented to the collection of the information from another source
- Collection of the information from another source would not prejudice a legitimate interest of the data subject
- Collection of the information from another source is necessary –
  - To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences
  - To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act34 of 1997
  - For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated
  - In the interests of national security, or
  - To maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied
- Compliance would prejudice a lawful purpose of the collection, or
- Compliance is not reasonably practicable in the circumstances of the particular case

7 Condition 3 - Purpose specification

Retention, destruction and restriction of records (section 14)

Summary of POPIA requirement

Retention

- Records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless –
  - Retention of the record is required or authorised by law
  - The responsible party reasonably requires the record for lawful purposes related to its functions or activities
  - Retention of the record is required by a contract between the parties thereto, or
  - The data subject, or a competent person where the data subject is a child, has consented to the retention of the record
  - The records of personal information is retained for historical, statistical or research purposes, provided that the responsible party has established appropriate safeguards against the records being used for any other purposes
- Further to the above, a responsible party that has used a record of personal information of a data subject to make a decision about the data subject must –
  - Retain the record for such period as may be required or prescribed by law or a code of conduct, or
  - If there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

Destruction/deletion/de-identification

- A responsible party must destroy or delete a record of personal information or deidentify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record in terms of POPIA.
- The destruction or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible form.
- Restriction
- The responsible party must restrict processing of personal information in certain circumstances set out in section 14(6) read with section 14(7) and section 14(8) of POPIA.

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity / project having regard to requirements above. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

8 Condition 4 - Further processing limitation

Further processing to be compatible with purpose of collection (section 15)

Summary of POPIA requirement

Further processing of personal information must be in accordance or compatible with the purpose for which it was collected in terms of section 13.

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity/project with regard to the requirements above. Note that section 15(2) of POPIA provides guidance regarding the factors to consider when assessing whether further processing is compatible with the original purpose of collection. Further, section 15(3) of POPIA gives examples of when further processing of personal information is not incompatible with the purpose of collection. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

9 Condition 5 – Information quality

Quality of information (section 16)

Summary of POPIA requirement

A responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary. In taking such steps, the responsible party must have regard for the purpose for which personal information is collected or further processed.

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity/project with regard to the requirements above. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

10 Condition 6 – Openness

Notification to data subject when collecting personal information (sections 17 and 18)

Summary of POPIA requirement

- A responsible party must maintain the documentation of all processing operations under its responsibility as required in terms of the Promotion of Access to Information Act.
- If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of the information specified in section 18(1).
- In this regard, the responsible party must take steps to make the data subject aware of the information –
  - If the personal information is collected directly from the data subject, before the information is collected, unless the data subject is already aware of the prescribed information, or
  - In any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity / project having regard to requirements above. Note that sections 18(3) and 18(4) of POPIA state when it is not necessary to comply with the transparency requirements of section 18(1) of POPIA and should be considered when assessing the risk of non-compliance. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

11 Condition 7 – Security safeguards

Security measures on integrity and confidentiality of personal information (section 19)

Summary of POPIA requirement

- A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent –
  - Loss of, damage to or unauthorised destruction of personal information, and
  - Unlawful access to or processing of personal information.
- In order to give effect to the above requirement, the responsible party must take reasonable measures to –
  - Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control
  - Establish and maintain appropriate safeguards against the risks identified
  - Regularly verify that the safeguards are effectively implemented, and
  - Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
- The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity / project having regard to requirements above. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

12 Condition 7 – Security safeguards

Security measures regarding information processed by operator (section 21)

Summary of POPIA requirement

A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 19 of POPIA.

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity/project with regard to the requirements above. It is recommended that a privacy due diligence is performed in respect of the operator to inform the risks identified in respect of the operator's ability to comply with the privacy and security requirements prescribed in terms of POPIA and any additional requirements prescribed by the responsible party. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

13 Condition 7 – Security safeguards

Notification of security compromises (section 22)

Summary of POPIA requirement

- Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify (a) the Regulator, and (b) subject to section 22(3) of POPIA, the data subject, unless the identity of such data subject cannot be established.
- Such notification must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity / project with regard to the requirements above. In considering the risks to compliance, the responsible party should also consider the subsections 22(3) to 22(5) of POPIA. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

14 Condition 8 – Data subject participation

Access to personal information (section 23)

Summary of POPIA requirement

- A data subject, having provided adequate proof of identity, has the right to –
  - Request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject, and
  - Request from a responsible party the record or a description of the personal information about the data subject held by the responsible party, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information, within a reasonable time; at a prescribed fee (if any); in a reasonable manner and format; and in a form that is generally understandable.
- A responsible party may or must refuse, as the case may be, to disclose any information requested by a data subject having regard to the grounds for refusal of access to records set out in the applicable sections of the Promotion of Access to Information Act, but then access to every other part of the record must be disclosed.

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity / project having regard to requirements above. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

15 Condition 8 – Data subject participation

Correction or deletion of personal information (section 24)

Summary of POPIA requirement

- On receipt of a valid request in terms of section 24(1) to correct, destroy or delete personal information, the responsible party must, as soon as reasonably practicable –
  - Correct the information as requested
  - Destroy or delete the information as requested
  - Provide the data subject, to his or her satisfaction, with credible evidence in support of the information, or
  - Where agreement cannot be reached between the responsible party and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.
- If the responsible party has taken steps that result in a change to the information pursuant to a request by the data subject, and the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, the responsible party must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of those steps.
- The responsible party must notify a data subject who has made a request of the action taken as a result of the request.

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity / project having regard to requirements above. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

PART E: RISKS RELATED THE TYPES OF PROCESSING

OVERALL RISK RATING FOR PART E	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

1 Processing activities

Processing activities

[Describe where personal information will be collected from, what processing is involved and what the purposes of processing are.]

Privacy risks identified

[Describe at a high level any privacy risks or special considerations that should considered in more detail having regard to the particular processing activities. Does the processing involve direct marketing, profiling or automated decision-making? What possible adverse impacts are there on the data subject as a result of the processing? Is the data subject likely to be aware of and expect the processing activities?]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

Direct marketing (section 69)

Summary of POPIA requirement

- The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication is prohibited unless the data subject –
  - Has given his, her or its consent to the processing,[19] or
  - Is a customer of the responsible party and the requirements of section 69(3)[20] of POPIA have been satisfied.
- Any communication for the purpose of direct marketing must contain details of the identity of the sender or the person on whose behalf the communication has been sent, and an address or other contact details to which the recipient may send a request that such communications cease.

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity / project with regard to the requirements above. Describe any areas of current non-compliance with the requirements.]

19 Section 69(2) states that a responsible party may approach a data subject whose consent is required and who has not previously withheld such consent, only once in order to request the consent of that data subject. Furthermore, the data subject's consent must be requested in the prescribed manner and form.

20 Section 69(3) states that responsible party may only process the personal information of a data subject who is a customer of the responsible party –

- If the responsible party has obtained the contact details of the data subject in the context of the sale of a product or service
- For the purpose of direct marketing of the responsible party's own similar products or services, and
- If the data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its electronic details –
  - At the time when the information was collected, and
  - On the occasion of each communication with the data subject for the purpose of marketing if the data subject has not initially refused such use

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

2 Directories (section 70)

Summary of POPIA requirement

- A data subject who is a subscriber[21] to a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which his, her or its personal information is included must be informed, free of charge and before the information is included in the directory (a) about the purpose of the directory and (b) about any further uses to which the directory may possibly be put, based on search functions embedded in electronic versions of the directory.
- A data subject must be given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its personal information or to request verification, confirmation or withdrawal of such information if the data subject has not initially refused such use.

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity / project having regard to requirements above. Describe any areas of current non-compliance with the requirements. Note that sub-sections 70(1) and 70(2) do not apply to editions of directories that were produced in printed or offline electronic form prior to the commencement of this section. Also consider if the exceptions contained in section 70(4) are applicable.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

3 Automated decision-making/profiling

(section 71)

Summary of POPIA requirement

A data subject may not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person (including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct), unless the decision –

- Has been taken in connection with the conclusion or execution of a contract, and
  - The request of the data subject in terms of the contract has been met, or
  - Appropriate measures[22] have been taken to protect the data subject's legitimate interests, or
- Is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.

21 Subscriber', for purposes of section 70, means any person who is party to a contract with the provider of publicly available electronic communications services for the supply of such services.

22 The appropriate measures must –
- Provide an opportunity for a data subject to make representations about the decision, and
- Require a responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information relating to him or her to enable him or her to make representations about the decision

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity/project with regard to the requirements above. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

4 Processing subject to prior authorisation (sections 57 to 59)

Summary of POPIA requirement

The responsible party must obtain prior authorisation from the Information Regulator, prior to any processing, if that responsible party plans to –

- Process any unique identifiers of data subjects –
  - – For a purpose other than the one for which the identifier was specifically intended at collection, and
  - – With the aim of linking the information together with information processed by other responsible parties
- Process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties
- Process information for the purposes of credit reporting, or
- Transfer special personal information or the personal information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information as referred to in section 72 of POPIA
- Perform any other types of processing which the Information Regulator has determined is subject to its prior authorisation in terms of section 57(2) of POPIA

Privacy risks identified

[Describe privacy risks identified in respect of the processing activity / project having regard to requirements above. Describe any areas of current non-compliance with the requirements.]

Mitigation measures to be implemented

[Describe mitigation measures in respect of the risks identified above.]

RISK RATING	Likelihood of risk	Severity of risk	Overall gross state risk	Overall residual risk
	[Inevitable, likely, or unlikely]	[Disastrous, moderate, negligible]	[High, medium, low]	[High, medium, low]

SAICA

THE SOUTH AFRICAN INSTITUTE
OF CHARTERED ACCOUNTANTS