ASISA GUIDELINES FOR RESPONSIBLE PARTIES ON THE PROTECTION OF PERSONAL INFORMATION ACT, 2013

Approved by the Regulatory Affairs BC on 7 July 2021

PART ONE – INTRODUCTION

1. DEFINITIONS AND INTERPRETATION

In the Guidelines, unless otherwise defined herein, terms will bear the meanings assigned to them in POPIA; and the following terms shall have the meanings assigned to them below:

1.1. **"ASISA"** means the Association for Savings and Investment South Africa;

1.2. **"Competent person"** has the meaning ascribed thereto in POPIA;

1.3. **"Guidelines"** means the guidance on the protection of personal information as contained in this document;

1.4. **"FAIS"** means the Financial Advisory and Intermediary Services Act, 2002;

1.5. **"FICA"** means the Financial Intelligence Centre Act, 2001;

1.6. **"FSRA"** means the Financial Sector Regulation Act, 2017;

1.7. **"PAIA"** means the Promotion of Access to Information Act, 2000;

1.8. **"POPIA"** means the Protection of Personal Information Act, 2013;

1.9. **"Product/s"** means the financial products (as defined in the FSRA) offered by the Responsible party;

1.10. **"Regulator"** means the Information Regulator established in terms of section 39 of POPIA;

1.11. **"Responsible party"** has the meaning ascribed thereto in POPIA and for purposes of the Guidelines means an ASISA member which is an institution referred to in clause 5 below; and

1.12. **"Service/s"** means the financial services (as defined in the FSRA) offered by the Responsible Party.

The **Guidance notes** and **Examples** provided for in the Guidelines are included to provide general guidance in respect of the application and interpretation of POPIA and the Guidelines only but are not prescriptive and shall have no binding legal force and effect.

2. BACKGROUND AND LEGISLATIVE BASIS

2.1. POPIA aims to give effect to the constitutional right to privacy by safeguarding personal information and regulates the way personal information must be processed, subject to justifiable limitations aimed at (i) balancing the right to privacy against other rights, particularly the right of access to information; and (ii) protecting important interests, including the free flow of information within South Africa and across international borders.

2.2. All ASISA members are committed to operating within the POPIA framework and conditions for processing of personal information. In seeking to comply with POPIA, ASISA members have developed the Guidelines as general principles to assist ASISA members in implementing POPIA.

2.3. Although the Guidelines set out standards of good practices relating to the processing of personal information and are intended to guarantee a uniform high level of information protection, individual Responsible parties must always ensure that they are compliant with the provisions of POPIA and/or any documents and guidance notes published by the Information Regulator.

2.4. In the event of any discrepancy or inconsistency between the Guidelines and POPIA, POPIA will prevail.

3. OBJECTIVES OF THE GUIDELINES

3.1. The main objective of the Guidelines is to promote high standards of behaviour and provide for, as practically as possible, a consistent approach on the part of Responsible parties in their efforts to address their handling of personal information, as envisioned in POPIA and by the Regulator.

3.2. The Guidelines aim to:

3.2.1 provide Responsible parties with principles which they should endeavour to meet in their dealings with data subjects and the processing of their personal information;

3.2.2 provide information to data subjects whose personal information is (or will be) processed by Responsible parties; and

3.2.3 contribute to the transparency of the principles applied in respect of the personal information processed and to be processed by Responsible parties.

4. APPLICATION OF THE GUIDELINES

4.1 The Guidelines set out a suggested framework for Responsible parties when processing personal information which falls within the scope of the Guidelines.

4.2 All Responsible parties are strongly encouraged to follow the Guidelines and to take all reasonable steps to implement the Guidelines effectively.

5. SCOPE

5.1. The Guidelines apply to the processing of personal information by the following Responsible parties:

5.1.1. a person who carries on "life insurance business" as defined in the Insurance Act, 2017;

5.1.2. a person who is authorised in terms of the Collective Investment Schemes Control Act, 2002 to administer collective investment schemes, excluding property unit trusts; and

5.1.3. category II (excluding brokers registered with the Johannesburg Stock Exchange), IIA and III Financial Service Providers as defined in FAIS.

5.2. Although registered pension fund administrators under section 13B of the Pension Funds Act, 1956 are acting primarily as operators for purposes of POPIA, where a person who is conducting such business also falls under the scope of the Guidelines in terms of clause 5.1, it will be expected of it as a best practice guideline to also comply with the Guidelines.

5.3. The Guidelines only apply to the processing[1] of personal information[2] of data subjects by Responsible parties, but only insofar as the processing is conducted within the ambit of their business activities as providers of Products and/or Services.

5.4. While all Responsible parties must comply with POPIA in respect of all personal information processing activities, the following processing of personal information by Responsible parties specifically falls outside the scope of the Guidelines:

5.4.1. the processing of personal information by Responsible parties in their capacity as employers;

5.4.2. the processing of personal information relating to suppliers, vendors, contractors or service providers of Responsible parties; and

5.4.3. the processing of personal information by Responsible parties in their capacity as operators[3] for other responsible parties.

Guidance notes

- A Responsible party is any "*person*" recognised in law i.e. natural or juristic persons. Companies within a group can be separately or jointly responsible for the processing of personal information.
- The definition of "*processing*" is very wide and will cover almost everything a Responsible party will do with personal information.
- When a Responsible party processes personal information on behalf of a Responsible party as an operator, the processing must be governed by a written contract with the Responsible party. However, the Responsible party remains accountable.

[1] See definition of "*processing*" in **Chapter 1**.
[2] See definition of "*personal information*" in **Chapter 1**.
[3] See definition of "*operator*" in **Chapter 1**.

PART TWO - CONDITIONS FOR PROCESSING PERSONAL INFORMATION

6. ACCOUNTABILITY

6.1. Responsible parties must ensure that the conditions set out in **Chapter 3** of POPIA, and in the Guidelines (subject to clause 4 above), and all the measures that give effect to such conditions, are complied with.[4]

7. INFORMATION OFFICER[5]

7.1. The Responsible party's information officer will be the head of the organisation or its delegate as contemplated in section 1 of PAIA and must register as such with the Regulator.

7.2. Each Responsible party may, if necessary, make provision for the delegation by the information officer of powers or duties to designated deputy information officers, and Deputy information officers must be registered as such with the Regulator.

7.3. The information officer must ensure that the Responsible party complies with the conditions for lawful processing of personal information under POPIA and, to the extent applicable, in the Guidelines. The information officer has the powers vested in him by POPIA and PAIA.[6]

Guidance note

In the context of group companies (and to the extent registered by the Regulator), the head of a subsidiary within the group may delegate the role of information officer to the same individual and register this individual with the Regulator so that the effect is that there is one information officer for a number of Responsible parties within the group.

[4] Section 8.
[5] See also: Guidance Note on Information Officers and Deputy Information Officers dd 1 April 2021 published by the Information Regulator: https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf
[6] Section 55.

PROCESSING LIMITATION

8. LAWFULNESS OF PROCESSING

8.1. Responsible parties must process personal information lawfully and in a reasonable manner that does not infringe the privacy of data subjects.[7]

Guidance note

When processing personal information, Responsible parties should not only comply with POPIA, but with the laws of South Africa in general, for example other statutes which may be applicable, the common law, and applicable industry codes of practice. If any other legislation provides for conditions for the lawful processing of personal information that are more extensive than those set out in POPIA or the Guidelines, the more extensive conditions prevail.

9. MINIMALITY

9.1. Responsible parties must not process personal information indiscriminately but only the minimum information they need to adequately fulfil the purpose for which it is being used.[8]

Guidance notes

- Responsible parties should check their methods of seeking information from data subjects on an ongoing basis to ensure that only relevant information is sought and provided.
- A Responsible party should not hold personal information on the off chance that it may be useful in the future.
- What is meant by "*adequate, relevant and not excessive*" in section10?
    - These words must be considered in the context of the purpose for which the personal information is being held and separately for each data subject or group of data subjects (where they share relevant characteristics). To assess whether a Responsible party is holding the right amount of personal information, the Responsible party must accordingly first establish why it is holding and using it.
    - Responsible parties may not process personal information which is superfluous to the purpose.
    - Personal information must also be sufficient - too little personal information may create an incorrect picture of the data subject.

Example

Do not collect details of marital status or race unless it is relevant to the Product or Services

[7] Section 9.
[8] Section 10.

being rendered or it is required in terms of legislation.

10. CONSENT, JUSTIFICATION AND OBJECTION

Grounds for processing

10.1. Responsible parties must always be able to base their processing on one of the grounds provided in section 11(1) of POPIA, otherwise they will not be allowed to process the personal information. Some of the relevant grounds are set out below.

Consent

10.2. A Responsible party may process personal information if the data subjects have consented to their personal information being collected and used in the manner and for the purpose in question. [9] [10]

Guidance notes

- Unless one of the other lawful grounds for processing applies, data subjects should be able to choose whether or not their personal information may be processed for a specific purpose.
- Consent must be specific. An unspecific (general) authorisation to process personal information which is not aimed at specific information and specific forms of processing will not be valid.
- Consent must be an expression of will, it must be voluntary, and it must be on an informed basis that points out to the data subjects, specifically, the scope of what they are consenting to as well as the consequences of consent.
- Consent must be capable of being withdrawn freely by data subjects.

10.3. The way in which consent is sought may vary, depending on the circumstances and the type of information, but an opt-in/express consent would be required for purposes of:

10.3.1. processing special personal information (see **clause 11** below); or

10.3.2. unsolicited electronic communication by means of direct marketing (see below).

Guidance note

To "opt-in" means that the data subjects must actively agree to the stated purpose, i.e. "opt in" or say "*yes*" to it, otherwise consent cannot be assumed.

Example

Opt-in: "*Please tick the box if you agree to receive marketing information from [ ]*".

[9] See definition of "*consent*" in **Chapter 1**.
[10] Section 11(1).

10.4. Responsible parties must:

10.4.1. obtain consent in a form appropriate to the circumstances;

Guidance note

Consent does not have to be in writing, but written consent is helpful in evidencing consent.

10.4.2. record the consent if verbal consent is obtained;

10.4.3. in obtaining consent, take the reasonable expectations of the data subjects into account; and

10.4.4. provide a convenient way for data subjects to withdraw consent and inform the data subjects of their right to withdraw consent. Responsible parties may not charge the data subjects for withdrawing their consent.

Guidance note

Responsible parties should inform data subjects of the consequences of withdrawing consent.

10.5. Consent for purposes of direct marketing by unsolicited electronic communications must be obtained in a form substantially similar to that contained in the POPIA regulations.

Guidance note

An opt-out provision may generally suffice in certain direct marketing scenarios. In these circumstances, to "opt-out" means that, unless the data subjects take action to "opt out" to the stated purpose, i.e. say "*no*" to it, consent may be assumed.

Example

Opt-out: "*Please tick the box if you do not want us to use your details for marketing purposes [ ].*"

10.6. Responsible parties must not, as a condition of the supply of a Product or Service, require data subjects to consent to the processing of their personal information beyond that required to fulfil the specified, legitimate purpose.

Necessary for performance of a contract

10.7. Responsible parties may process personal information if it is necessary to conclude or perform in terms of a contract to which the data subjects are party.[11]

[11] Section 11(1)(b).

Guidance notes

- Processing has to be a necessary consequence of the contract.
- Even if a Responsible party is not party to the contract, but it is necessary that the Responsible party processes personal information for the performance of a contract between the data subjects and another party this processing is allowed, for example cessions or underwritten retirement annuities.

Example

A Responsible party processes information contained in an application for an insurance or investment contract.

Legal obligation

10.8. A Responsible party may process personal information if such processing complies with an obligation imposed by law on the Responsible party.[12]

Guidance note

Before providing information to third parties, Responsible parties must check whether the request for information is lawful.

Examples

- Processing conducted by a Responsible party in order to comply with FICA.
- Personal information provided to the various regulators or public bodies in terms of applicable legislation.
- Personal information provided to the various Ombud schemes.
- Processing conducted to comply with court orders or subpoenas.
- Personal information provided to SARS in terms of the Income Tax Act.
- Medical information relating to exposure to or contamination by an infectious disease which is a notifiable disease as prescribed.

[12] Section 11(1)(c)

Legitimate interest of the data subjects

10.9. Responsible parties may process personal information if the processing protects a legitimate interest of the data subject.[13]

Guidance note

A Responsible party should conduct legitimate interest assessments that consider the necessity of the processing, balancing same with the interests of the data subject and implementing the necessary safeguards protecting the privacy of the data subject.

Examples

- A Responsible party may provide contact details of a client of one of its representatives to another of its representatives (within the same Responsible party) on the termination of the first representative's contract in order to ensure proper financial care for the client.
- A Responsible party is unable to locate a beneficiary to whom a payment must be made and discloses the beneficiary's details to a tracing agent to find the beneficiary.
- A Responsible party is required to trace "dependants" as defined in the Pension Funds Act.
- A Responsible party may process the personal information of a person appointed as a beneficiary on a policy.
- A Responsible party may process the personal information of clients where the processing is necessary for the prevention and detection and remediation of (suspected) fraud or other misconduct.
- A Responsible party may process personal information about potential clients in order to conduct an affordability test.

Public law duty

10.10. Personal information may be processed if such processing is necessary for the proper performance of a public law duty by a public body.[14]

Guidance note

Before providing information to a public body, Responsible parties must check whether a public law duty exists.

[13] Section 11(1)(d).
[14] Section 11(1)(e).

Example

If the police request information from a Responsible party regarding one of the Responsible party's customers in connection with an investigation, the Responsible party would be allowed to share the information with the police.

Legitimate interest of the Responsible party or third party

10.11. Responsible parties may process personal information if this is necessary to pursue the legitimate interests of the Responsible party concerned or a third party to whom the information is supplied unless such interests are overridden by the interests of the data subjects.[15]

Guidance notes

- POPIA recognises that there may be legitimate reasons for processing personal information that the other conditions for processing do not specifically deal with. This "legitimate interest" condition permits such processing, provided that it does not prejudice the rights of the data subject.
- The term "*necessary*" means that the condition will not be met if the Responsible party can achieve the purpose by some other reasonable means or if the Responsible party decides to operate its business in a particular way.
- Legitimate interest should be assessed to achieve a balance between:
  - The interests of the data subject; and
  - The interests of the Responsible party or third party.
- In assessing legitimate interest, the steps that should be considered in this balancing test are:
  - Assessing the responsible party's or third party's interest;
  - The impact on the data subject's interest;
  - The provisional balance of interests;
  - The effect of any additional safeguards implemented to prevent undue impact on the data subjects;
  - The final assessment.
- In assessing a Responsible party's interest, cognisance must be taken of the qualifying action. POPIA variously requires a legitimate interest be protected, pursued, maintained, etc. The qualifying action indicates parameters for weighing the extent of the intrusion into the privacy of the data subjects and whether this is justified.
- The impact on the data subjects should take into account factors such as the type of personal information, the reasonable expectations of the data subjects around use of the data and the power differential between the parties.

[15] Section 11(1)(f).

- The provisional balance is assessed to understand whether further safeguards should be implemented to protect the privacy of the data subjects. Once those further steps, if any, are in place, the balance is assessed again.
- It is recommended that Responsible parties document assessments of legitimate interest.

Examples

- Processing is necessary for the prevention, the detection or investigation, and remediation of (suspected) fraud or other misconduct.
- Processing is necessary for the sound management of a Responsible party's business. Legitimate interests are not limited to core activities. This may include processing of personal information to ensure efficient servicing of clients.
- Processing for risk mitigation.

Objection by the data subjects to processing[16]

10.12. Data subjects may object on reasonable grounds to processing conducted on the grounds mentioned in clause 10.9 (legitimate interest of data subjects), 10.11 (legitimate interest of Responsible party or third party) and 10.10 (public law duty) above, unless legislation provides otherwise[17].

Guidance note

Once data subjects have registered an objection, the Responsible party should judge whether the objection is reasonable. If that is the case, the relevant Responsible party must end the processing immediately.

Examples

The following are examples of instances where an objection to processing would not be considered reasonable:

- where the Responsible party is performing its obligations in terms of a contract; or
- where the Responsible party is exercising its rights in line with agreed terms of a contract.

11. PROCESSING OF SPECIAL PERSONAL INFORMATION[18]

Prohibition on processing of special personal information

11.1. Some personal information is sensitive information, and the processing thereof can

[16] Section 11(3).
[17] Section 11(3).
[18] See also: Guidance Note on Special Personal Information dd 28 June 2021 published by the Information Regulator: https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-Processing-SpecialPersonalInformation-20210628.pdf

constitute a significant or substantial intrusion of the data subjects' privacy and is prohibited unless a general or special exemption applies.

11.2. POPIA refers to the following information as "**special personal information**"[19]:

11.2.1. information concerning data subjects' religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information and criminal behaviour.

11.3. The processing of special personal information is subject to a stricter regime than the processing of ordinary personal information. POPIA provides certain general and special exemptions from the prohibition to process special personal information.

General exemptions

11.4. The general exemptions apply to the processing of any special personal information.

11.5. The general exemptions allow for the processing of special personal information[20]:

11.5.1. with the consent of the data subjects. Note that consent in the case of special personal information must be explicit, i.e. the data subjects must have expressed their will explicitly – refer to section on **consent** above;[21]

Examples

- Disclosure of religious information in connection with products where religion is relevant.
- Disclosure of health-related risks with regard to lifestyle programmes.

11.5.2. if it is necessary to establish, exercise or defend a right or obligation in law;[22]

Examples

- Responsible parties may have to disclose information about data subjects in legal proceedings in order to be able to defend their own position, e.g. when there is a dispute regarding the non-disclosure of medical information in a policy application form.
- Political information or criminal information required for FICA purposes.
- Responsible parties may have to disclose information about data subjects in line with a court order.
- Responsible parties may have to disclose information about data subjects in line with a request from regulators (including the Information Regulator) or dispute resolution authorities.

[19] See section 26.
[20] Section 27.
[21] Section 27(1)(a)
[22] Section 27(1)(b).

11.5.3. If the processing is necessary to comply with an obligation of international public law;

11.5.4. if the Regulator granted authority in terms of section 27(2) of POPIA and appropriate guarantees have been put in place to protect the data subjects' privacy;

11.5.5. if the processing is for historical, statistical or academic or scientific research purposes to the extent that:

11.5.5.1. the purpose serves a public interest and the processing is necessary for that purpose, or

11.5.5.2. it appears to be impossible or would involve a disproportionate effort to ask for consent,

and sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the data subjects to a disproportionate extent;[23]

11.5.6. if the information has deliberately been made public by the data subjects; or

11.5.7. provisions of sections 28 to 33 of POPIA are, as the case may be, complied with.

Guidance note

The intention of the data subjects to make the information public has to be clear and it should be utilised in accordance with the intention of the data subjects (e.g. addresses for telephone directories).

Special exemptions

11.6. In addition to the general exemptions certain special exemptions apply in respect of different types of special personal information.

Religious or philosophical beliefs[24]

11.7. In brief, the ban on processing information about someone's religious or philosophical beliefs does not apply to church associations or other associations founded on spiritual principles or other associations founded on philosophical principles.

Guidance note

Responsible parties will not be able to process religious information under this exemption and will need to obtain explicit consent or process religious information under one of the general exemptions. Shariah / Islamic investments are typically processed with the consent of the data subjects and hence processing of such religious beliefs by Responsible parties

[23] Section 27(1)(d).
[24] Section 28.

will be allowed.

11.8. Responsible parties may never provide information about a person's religious or philosophical beliefs to third parties without the data subjects' consent.

Race[25]

11.9. Personal information about data subjects' race may only be processed when it:

11.9.1. is to identify data subjects, but only where this is essential for that purpose; and

11.9.2. is carried out to protect or advance those disadvantaged by unfair discrimination.

Example

BEE / employment equity reporting purposes.

Political persuasion[26]

11.10. Personal information about data subjects' political persuasion may broadly speaking only be processed by institutions founded on political principles if it is necessary to form a political party or canvas supporters or votes for a political party or campaign for a political party or cause.

Guidance note

Responsible parties will not be able to process political information under this exemption and will need to process political information under one of the general exemptions.

Trade Union Membership[27]

11.11. Only Trade Unions may process personal information concerning trade union membership and may not disclose such information to anyone without the member's consent.

Guidance note

Responsible parties should check that the trade union has the members' consent to disclose their information and would be well advised to obtain an indemnity from the trade union in this regard.

Health or sex life[28]

11.12. Information about a person's health or sex life includes all data concerning the mental or physical health of a person.

[25] Section 29.
[26] Section 31.
[27] Section 30.
[28] Section 32.

Example

Information relating to pregnancy, sexual orientation, physical or mental health, well-being, disability, birth, medical history, or blood type.

11.13. POPIA names a number of groups of Responsible parties that may, under certain conditions, process personal information about a person's health, but only for specific purposes. The prohibition on processing personal information concerning a data subjects' health or sexual life does *inter alia* not apply to processing by:

11.13.1. Insurance companies, medical aid schemes, medical aid scheme administrators and managed health care organisations, if such processing is necessary for:

11.13.1.1. assessing the risk to be insured by the insurance company or covered by the medical scheme and the data subjects have not objected to the processing;

11.13.1.2. the performance of an insurance or medical scheme agreement; or

11.13.1.3. the enforcement of any contractual rights and obligations;[29]

Guidance note

More detailed rules may be prescribed in respect of this processing.

Example

A Responsible Party processes a data subject's health or sex life information to assess the risk to be insured by the insurer, perform an insurance contract and/or enforce contractual rights and obligations.

11.13.2. administrative bodies, pension funds, employers or institutions working for them if such processing is necessary for:

11.13.2.1. the implementation of the provision of laws, pension regulations or collective agreements which create rights dependent on the health or sexual life of the data subjects; or

11.13.2.2. the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.[30]

11.14. POPIA requires that the Responsible party processing the information is bound by a duty of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the Responsible party and the data subjects.[31]

[29] Section 32(1)(b)
[30] Section 32(1)(f).
[31] Section 32(2) and (3).

11.15. The processing of personal information relating to data subjects' state of health that can be derived from a blood test is also subject to the **ASISA HIV Testing Protocol**.

11.16. Personal information concerning inherited characteristics may not be processed in respect of the person from whom it was collected, unless a serious medical interest prevails, or the processing is necessary for historical, statistical or research activity.

Guidance note

If a data subject provides an insurer with data on hereditary characteristics about himself for taking out life insurance, these hereditary characteristics may only be used in connection with that person himself and not in connection with family members to whom the information necessarily relate as well.

Criminal behaviour or biometric information[32]

11.17. The prohibition on processing personal information concerning data subjects' criminal behaviour or biometric information does not apply if:

11.17.1. the processing is carried out by bodies charged by law with applying criminal law; or

11.17.2. the information has been obtained in accordance with the law;

Examples

- SARS appoints the Responsible party to act as its agent to provide information on data subjects to SARS for purposes of tax evasion.
- To comply with FICA's money laundering obligations.
- Information is obtained in terms of a court order.
- Compliance with FAIS with regard to fit and proper evaluations.

12. PROCESSING OF PERSONAL INFORMATION OF CHILDREN[33]

Prohibition on processing personal information of children

12.1. A Responsible party may not process personal information concerning a child unless a general authorisation applies.

12.2. POPIA defines a child as a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person[34], to take any action or decision in respect of any matter concerning him or herself.

---

[32] Section 33.
[33] See also: Guidance Note on processing of personal information of children dd 28 June 2021 published by the Information Regulator: https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-Processing-PersonalInformation-Children-20210628.pdf
[34] See definition of "*competent person*" in **Chapter 1**.

General authorizations

12.3. The following general authorisations allow for the processing of personal information of children:[35]

12.3.1. Processing is carried out with the prior consent of a competent person[36]. Note that consent in the case of special personal information must be opt-in consent, i.e. the data subjects must have expressed their will explicitly – refer to section on **consent** above;[37]

12.3.2. if it is necessary to establish, exercise or defend a right or obligation in law;[38]

Examples

- Determining whether children are entitled to benefits in terms of legislation or contract (for example, whether children may be insured based on an insurable interest).
- Tracing children who are entitled to benefits in terms of a financial product.

12.3.3. It is necessary to comply with an obligation of international public law;

12.3.4. if the Regulator granted authority in terms of section 35(2) of POPIA;

Example

When someone other than a competent person (as defined) supplies personal information relating to children in order for a Responsible party to process such information, an exemption may have to be applied for.

12.3.5. if the processing is for historical, statistical or research purposes to the extent that:

12.3.5.1. the purpose serves a public interest and the processing is necessary for that purpose; or

12.3.5.2. it would involve a disproportionate effort to ask for consent,

and sufficient guarantees are provided to protect the privacy of the data subjects;[39]

12.3.6. if the information has been deliberately made public by the child with the consent of a competent person.

Guidance note

The intention of the data subjects to make the information public has to be clear and it should be utilised in accordance with the intention of the data subjects (e.g. addresses for

[35] Section 35
[36] Section 35((1)(a).
[37] Section 35(1)(a)
[38] Section 35(1)(b).
[39] Section 35(1)(d).

telephone directories)

13. COLLECTION DIRECTLY FROM DATA SUBJECTS

13.1. Responsible parties must collect information directly from the data subjects except where POPIA specifically allows collection from other sources.[40]

13.2. Collection from other sources is allowed[41]:

13.2.1. where the information is contained in or derived from a public record or has deliberately been made public by the data subjects;

Guidance notes

- "Public domain" is not necessarily a "public record". See definition of "*public record*" in Chapter 1 of POPIA.
- Whether information has been deliberately made public will depend on the purpose for which it is published. Telephone directory information should, for example, not be regarded as information contained in a "*public record*" or that has been "*deliberately made public*". Data subjects expect their information to only be used for the purposes they added their information to the directory. Responsible parties should not misuse the information printed in the directory, for example to conduct unsolicited marketing calls.

13.2.2. where the data subjects (or a competent person where the data subject is a child) have consented to the collection of the information from another source;

13.2.3. where collection from another source would not prejudice the legitimate interests of the data subjects;

Examples

- Where information is obtained to locate/contact a beneficiary under a claim.
- Policyholders providing information on lives assured or third-party beneficiaries.
- Verification of the data subjects' contact details.
- Joint life insurance and key person or contingent liability insurance.

13.2.4. where collection of the information from another source is necessary to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue (as defined in the South African Revenue Service Act, No 34 of 1997);

Examples

- Information collected in the process of independent verification in terms of FICA.

[40] Section 12(1).
[41] Section 12(2).

- Information collected to comply with the FAIS fit and proper requirements.

13.2.5. for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

13.2.6. in the interests of national security; or

13.2.7. where collection from another source is necessary to maintain the legitimate interests of the responsible party or a third party.

Guidance note

Where information may be sought from industry data bases, credit bureaux or other sources to verify independent information provided by the data subjects or to combat fraud, Responsible parties should disclose the fact that the information will be sought and the purpose for which it will be sought to the data subjects. However, where information is requested from a credit bureau for assessing an application for insurance, regulation 18(5) of the National Credit Act states that the consent of the consumer must be obtained prior to the report being requested. It is not sufficient to merely disclose that the information will be requested.

Examples

- Collection from data bases through which information about medical impairments and claims are shared to combat fraud, such as industry registers (for example the applicable industry Life & Claims Register).
- Collection from credit bureaux for fraud prevention, verifying information or tracing consumers.
- A Responsible party may process personal information about potential clients in order to conduct an affordability test (depending on the source – see Guidance Note below).

13.2.8. where compliance would prejudice a lawful purpose of the collection; or

Guidance note

Where information has not been collected directly from the data subjects because it would prejudice a lawful purpose, the Responsible party may not use the information so collected for any purpose unrelated to the specific purpose used to obtain the exemption in question.

Example

Collection from other sources for purposes of conducting a lawful forensic investigation.

13.2.9. Where compliance is not reasonably practicable in the circumstances of the particular case.

Guidance note

Where information has not been collected directly from the data subjects because it would not be reasonably practicable in the particular case, the Responsible party may not use the information so collected for any purpose unrelated to the specific purpose used to obtain the exemption in question.

13.3. Where a Responsible party buys any data base which contains data subjects' personal information, the Responsible party may only use the personal information for the purpose/s for which it was consented to by the data subjects.

Guidance notes

- Responsible parties should establish what the purposes are for which the seller collected the information when they buy the data base and for which purposes the data subjects had provided consent, including ensuring that the data subjects provided consent to the selling of their information. If a Responsible party wants to use the personal information for any other purposes, it will have to get consent for this from the data subjects.
- It is good business practise to put a data sharing agreement in place with the seller of a data base that covers, inter alia, warranties by the seller that it is sharing the data in accordance with the lawful conditions for processing in POPIA, and that it has received the necessary consent and made the necessary disclosures to the data subjects to indicate that it intends to sell the data subjects' information.

13.4. If a Responsible party intends to contact data subjects after having obtained a lead via word of mouth, they must first seek the data subject's consent to be contacted before they are allowed to further use the information.

Guidance note

It is good business practise to record the details of the person / institution providing the lead. Section 18 of POPIA also requires that a data subject is made aware of the source of data collection when not collected directly from the data subject.

Example

When telephoning the data subjects based on a lead, the person representing the Responsible party must first ask the data subjects if they may talk to them about the new Product or Service that can be offered.

13.5. Where someone applies for a Product on behalf of another person, personal information is not collected directly from the data subjects. The person is in this case deemed to be acting on behalf of the data subjects and is therefore deemed to have obtained the consent of the data subjects.

Examples

- Third party beneficiaries of insurance products.

- Joint life insurance.
- Key man person, contingent liability, loan account cover insurance and any company owned policy.
- A person applies for policy benefits where a third party is the life assured.

Guidance note

The information requirements towards the data subjects imposed by POPIA can be directed to a person acting on behalf of the data subjects. It is recommended that a person acting on behalf of a data subject is asked to warrant that he/she has the permission of the data subject to act on their behalf and to therefore provide the personal information of the data subject.

PURPOSE SPECIFICATION

14. COLLECTION FOR A SPECIFIC PURPOSE

Specify the purpose clearly

14.1. Responsible parties must specify the purpose for which they obtain personal information[42].

Guidance notes

- This requirement aims to ensure that Responsible parties are transparent about their reasons for obtaining personal information and that what they will do with the information is in line with the reasonable expectations of the data subjects.
- Statements of purpose should not be so broad as to make this condition meaningless e.g. "*to serve you better*" or "*for your benefit*".
- Purposes should be specified in such a manner that the data subjects can reasonably understand why the information is being collected and how it will be used.
- Responsible parties should further process information only in a way that is compatible with the original purpose.

Examples

- Examples of processing by Responsible parties include, but are not limited to:
  - the provision of Services;
  - the issue of Products, for example a life insurance policy, a participatory interest in a collective investment scheme;

[42] Section 13.

- the assessment and processing of any claims arising in terms of Products;
- the provision of policy loans;
- the rendering of intermediary services in respect of financial products through bulking;
- compliance with statutory or regulatory obligations or other obligations imposed by law;
- the assessment of risk in issuing financial products;
- the provision of associated services such as wills and financial plans; and
- providing information to data subjects who requested to receive such information.

- Examples of further processing by Responsible parties include, but are not limited to:
  - the direct marketing of Products (to the extent not specified in the original purpose) to existing and potential customers (see section on Direct Marketing below for guidance);
  - direct marketing by Product Suppliers to intermediaries who place business with them via third-party platforms where it is the reasonable expectation of the intermediary to receive direct marketing communications from the product supplier;
  - cross selling (to the extent not specified in the original purpose) (see section on Direct Marketing below for guidance); and
  - profiling (see section on Profiling/Statistical Analysis for guidance).

Notification to data subjects

14.2. Responsible parties must notify the data subjects of the purposes of collection[43] [44] unless one of the exemptions applies.[45]

Guidance note

See section on **Openness** below.

RETENTION OF RECORDS

Balancing the right to privacy with the right of access to information

Guidance notes

- POPIA's stated purpose is to give effect to the right to privacy subject to justifiable limitations that are aimed at balancing this right against other rights, particularly the right of access to information. The provisions of POPIA, and in particular the

[43] Section 13(2).
[44] Section 18(1).
[45] Section 18(4).

requirements in section 14, need to be interpreted in a manner that gives effect to the purpose of POPIA, whilst maintaining the right to access to information. There will need to be a balance between the prevention of indefinite retention of data vs entities being required to retain data to be able to fulfil products, services or for legal or regulatory purposes, or the ability to exercise any powers, duties, and functions in terms of the law insofar as processing of information is concerned.

- ASISA members are in the vanguard of fighting financial crime, most notably: money-laundering, terrorist-financing, fraud and corruption. One of the tools at Responsible parties' disposal to step up the fight against financial crime is data. Data collected by banks, financial services companies and public institutions is often the evidentiary trail to assist law enforcement authorities in the detection, investigation, prosecution, and confiscation of criminal funds where illicit activities are concerned.
- It is therefore prudent for ASISA members to proceed cautiously prior to launching extensive record destruction programmes and to take into account relevant statutory periods, contractual periods and the requirements of various regulatory bodies that may require data be held for longer periods of time.

How long must records be kept for?

14.3. Responsible parties must not keep personal information for longer than is necessary for achieving the purpose for which it was collected (or further processed).

Guidance notes

- How long personal information should be kept depends on the purpose for which it was obtained and further processed, and its nature. This may be different in every situation.
- In order to give effect to this principle, Responsible parties will need to:
  - review the length of time they keep different types of personal information;
  - consider the purposes the different types of personal information are being held for in deciding whether and for how long to retain it;
  - securely delete and/or safeguard and/or anonymize information (as applicable) that is no longer needed for those purposes; and
  - update, archive or securely delete information if it goes out of date.
- Determining retention periods is ultimately a matter of risk management. Responsible parties must make their own risk assessment around the retention and disposal of records.
- It is good practice to establish standard retention periods for different categories of information and to have a system in place for ensuring that the Responsible party keeps to these retention periods.
- Always taking into account the balance between a data subject's right to privacy and the right of access to information, a Responsible party should not hold personal information on the off chance that it may be useful in the future.
- See section 14.4.2 for further guidelines on how to store information that is retained for

a longer period of time.

Exceptions

14.4. Information may be kept for longer than required for the purpose collected if:[46]

14.4.1. retention of the record is required or authorised by law;

Guidance notes

- In determining appropriate retention periods, regard must be had to statutory retention periods and obligations imposed on the Responsible party. Various statutes prescribe how long information must be held (with some even requiring that information should be held indefinitely) (see Examples below).
- There are various other legal requirements, applicable codes of conduct and professional guidelines about keeping certain kinds of records, for example for tax and audit purposes.
- The legal and commercial implications should the document be destroyed must be considered.
- See section 14.4.2 for further guidelines on how to store information that is retained for a longer period of time.

Examples

- FICA sections 22, 23 and Guidance Note 7. Records must be kept for at least 5 years from the date on which the business relationship is terminated.
- Section 24 of the Companies Act, 2008 requires records to be kept for 7 years. Certain records are required to be kept for an indefinite period.
- FAIS provides in section 18 which records must be kept for 5 years.
- The Prescription Act, 1969, section 11c. For safety reasons, documents should be kept longer than the periods laid down in this act. The periods may also be extended as a result of interruption or suspension of prescription.
- The Collective Investment Schemes Control Act, 2002, section 54.
- The Pension Funds Act, 1956, section 30L.
- The Tax Administration Act, 2011, sections 29, 32 and 99 (where certain records must be retained indefinitely).
- The Income Tax Act, 1962, 4th and 6th Schedules.

For more guidance on statutory retention periods, see the SAICA Guide on the Retention of Records at Guides (saica.co.za).

14.4.2. the Responsible party requires the record for lawful purposes related to its

[46] Section 14(1).

functions or activities;

Guidance notes

- When personal information is required to be kept in such circumstances (i.e. for longer than required for the purpose), it is recommended that such personal information be isolated from the Responsible party's general systems i.e. safe-guarded and ring-fenced (which may include encoding and/or anonymizing the information) from general access by employees. Only a limited group of authorised employees should be able to access such data and only for a valid purpose (as outlined above and set out in the Examples). Responsible parties should not use this as a blanket justification to hold all personal information on the off chance that it may be useful in the future but must constantly weigh up the rights of the data subjects to the privacy of their information versus the need to retain the information.
- Responsible parties must use best endeavours to appropriately safeguard the information from being used for any other purpose.

Examples

- Where data subjects propose for but do not subsequently proceed with a financial transaction, or it is declined, details may be kept on file for a limited period to facilitate a subsequent application, enquiries, complaints or as a check against non-disclosure.
- Responsible parties may need to keep personal information about a customer so that they can deal with possible complaints about the services provided by the Responsible parties.
- If a Responsible party receives a notice from a former customer requiring it to stop processing the customer's personal information for direct marketing, it is appropriate for the Responsible party to retain enough information about the former customer for it to stop including the person in future direct marketing activities.
- In some cases, a Responsible party may need to keep personal information so that it can defend possible future legal claims. Statutory prescription periods may be useful to determine retention periods.
- Responsible parties may need to keep personal information for the prevention of fraud, money laundering, terrorist-financing, corruption and other illicit financial crime purposes. This may include tax fraud/evasion and/or other investigations by SARS requiring personal tax information of data subjects.
- Claims involving pension funds where the PFA insists on viewing a client's retirement history (which could be a 20 to 30-year period).
- Commissions of inquiry occur frequently in SA and require data from financial institutions as part of their investigations, often going back several decades.
- See further Examples under 14.4.1 above.

14.4.3. retention of the record is required by a contract between the parties thereto;

14.4.4. the data subject or a Competent person where the data subject is a child has

consented to the retention of the record;

Examples

- To track beneficiaries for unclaimed benefits.
- For claims involving minor children that may require follow up at a later date.
- For insurance claims and underwriting purposes.

14.5. Records kept for historical, statistical or research purpose may also be kept longer than the purpose it was collected for, provided that the Responsible party has established appropriate safeguards against the information being used for any other purposes.[47]

14.6. If a Responsible party has used the data to make a decision about data subjects, the information must be kept for a period as may be required by law or a code of conduct, or if there is no law or code of conduct, for a period which will afford the data subjects a reasonable opportunity to request access to the record[48].

Examples

Where decisions are made:

- In terms of FICA.
- Based on the applicable industry Life and Claims Register.
- For insurance claims and underwriting purposes.
- In terms of SARS and the Income Tax Act and related tax legislation.

14.7. Once a Responsible party may no longer hold personal information, the Responsible party must destroy, delete or de-identify[49] the information as soon as reasonably possible.[50]

Guidance notes

- Destruction or deletion must be such that any reconstruction is prevented.
- It is advisable to keep an audit trail of acquisition, use and destruction of personal information.

Data Retention Policies

14.8. It is good practice to have a data retention policy.

[47] Section 14(2).
[48] Section 14(3)
[49] See definition of "*de-identify*" in **Chapter 1**.
[50] Section 14(4).

Guidance notes

- A data retention policy weighs legal and privacy concerns against economics and need-to-know concerns to determine the retention time, archival rules, data formats, and the permissible means of storage, access, and encryption.
- Data retention policies should deal *inter alia* with:
  - best practice for the key type of records identified therein;
  - the different purposes for which the Responsible party holds personal information and the length of time that such information should be retained for those purposes;
  - classification of records, document management processes, special safeguarding capabilities;
  - applicable regulatory requirements relevant to retention;
  - the procedure for archiving the information, guidelines for destroying the information when the time limit has been exceeded;
  - the safe storing/archiving of information which does not need to be accessed regularly but still needs to be retained;
  - special mechanisms for handling the information when under litigation;
  - auditing of the policy.
- Do not be inconsistent in policing/enforcing the policy. This can lead to allegations of discriminatory treatment.
- There is a tangled web of potentially relevant laws so Responsible parties must take care not to infringe the law.

FURTHER PROCESSING LIMITATION

15. COMPATIBLE PURPOSE

Further processing must be compatible with original purpose of collection

15.1. Responsible parties may process personal information only if such processing is compatible with the original purpose for which it was collected.[51] [52]

[51] See section 15(2) for factors to take into account to assess whether further processing is compatible.
[52] See section 15(3) for processing which is not incompatible with the purpose of collection.

Guidance notes

- Whether further processing is compatible will depend on the circumstances. Sections 15(2) and (3) specify to some extent what is meant by compatibility.
- In determining compatibility, Responsible parties should also take into account the reasonable expectations of the data subjects and any adverse effects on the data subjects.

If further processing is necessary to comply with an obligation imposed on a Responsible party by law, the processing will not be incompatible with the original purpose of collection.

Examples

- Information requested lawfully by the Financial Sector Conduct Authority (FSCA), the Prudential Authority, SARS or FIC or any other applicable regulatory body.
- Persons to whom Responsible parties are authorised to disclose personal information, in addition to the legal obligation to process referred to above include:
  - relevant ombudsmen or equivalent complaints bodies or alternative dispute adjudicators; and
- persons appropriately authorised to act on behalf of the data subjects, such as directors, curators, executors or trustees or agents

Direct Marketing

15.2. The question of whether it is permitted to process personal information for direct marketing purposes must be assessed using the general lawful conditions for processing personal information. This means, amongst other things, that processing for direct marketing purposes may *not be incompatible* with the purpose for which the information was obtained. If the personal information was acquired for direct marketing purposes, the processing for that purpose is of course compatible.

15.3. See section on **Direct Marketing** below.

16. INFORMATION QUALITY

16.1. Responsible parties must take reasonably practical steps to ensure that personal information is complete and accurate and updated where necessary, having regard to the purposes for which the personal information is collected or further processed.[53]

[53] Section 16.

Guidance notes

- Whether or not to keep personal information up to date will depend on what the information will be used for. If the information is used for a purpose that relies on it remaining current, it should be kept up to date. If not, for example when information is only stored, it will not be necessary to keep the information up to date.
- Ensuring information quality should be a continuous process and regard should be had to generic data quality management processes, e.g. define, assess, remediate and monitor.
- It may be impractical to check the accuracy of personal information provided by someone else. A Responsible party will not be in breach of this principle as long as the Responsible party has accurately recorded the information and has taken reasonable steps to ensure the accuracy. Reasonable steps will include requesting clients to keep their information updated during normal client interactions.

OPENNESS

17. NOTIFICATION TO THE REGULATOR

17.1. The Responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 51 of PAIA.[54]

18. NOTIFICATION TO THE DATA SUBJECTS

18.1. Responsible parties must be transparent about their reasons for obtaining personal information and must ensure that what they do with the information is in line with the reasonable expectations of the data subjects.

18.2. When personal information is collected, the Responsible party must take reasonably practicable steps to ensure that the data subjects are aware of:[55]

18.2.1. the information being collected and where the information is not collected from the data subjects, the source from which it is collected;

18.2.2. the name and address of the Responsible party;

18.2.3. the purpose for which the information is being collected;

18.2.4. whether or not the supply of the information by the data subjects is voluntary or mandatory;

18.2.5. the consequences of a failure to provide the information;

18.2.6. any particular law authorising or requiring the collection of information;

18.2.7. the fact that, where applicable, the Responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international

[54] Section 17
[55] Section 18(1).

organisation;

18.2.8. the recipients or category of recipients of the information;

18.2.9. nature or category of the information;

18.2.10. existence of the right of access to and the right to rectify the information collected;

18.2.11. existence of the right to object to the processing of personal information as specified in POPIA;

18.2.12. right to lodge a complaint to the Regulator and the contact details of the Regulator; and

18.2.13. any further information which is necessary under the specific circumstances to ensure reasonable processing.

Guidance notes

- Further information which may be relevant for purposes of clause 18.2.13 includes the recipients of the information, the nature of the information and the existence of the right of access to and the right to rectify the information.
- Each Responsible party should have a written privacy notice setting out for what purposes personal information is collected and further processed and ensure that the notice appears on websites or documentation where personal information is collected.
- Remember that informed consent will ultimately depend on the data subjects' knowledge of what they are consenting to.[56]
- Disclosures should be made in plain and understandable language as contemplated in section 22 of the Consumer Protection Act, 2008.
- When specifying purposes orally, Responsible parties should:
  - explain the purposes to data subjects in a clear and consistent manner; and
  - if it records telephone calls with data subjects (e.g., for quality control purposes), inform the data subjects of this practice and its purposes at the beginning of every call.
- Responsible parties have to ask themselves if it is necessary, for reasons of due care, to provide more (or more detailed) information to the data subjects about the processing. If the information falls under the category of special personal information, there will probably be more reason to provide detail.
- Responsible parties should explain to the data subjects what the consequences are of failing to provide the information, for example where a credit check is necessary in order to issue the product or information is necessary to process a claim.
- Even if information is exempted from the notification requirement, anyone may still request a Responsible party to provide information about it.

[56] See section on **Consent** above.

18.3. If information is collected from the data subjects, the Responsible party must inform the data subjects prior to the collection, unless the data subjects are already aware of the information.

18.4. If information is not collected directly from the data subjects, the data subjects must be notified before collection, or as soon as reasonably practicable after it has been collected.

Guidance notes

- If it concerns a limited number of data subjects, Responsible parties must inform them personally. If it concerns a whole group, Responsible parties may limit themselves to a more general form of providing information, for example in a bulletin, provided that it is certain that it will reach the entire group of data subjects. Placing an advertisement in a newspaper is not enough.
- It is recommended that Responsible parties retain an audit trail of acquisition of personal information.

Example

Where data subjects are third party claimants who would not otherwise have received a notice, an appropriate privacy notice must be made available at a suitable point in the business process, e.g. a claims procedure document.

18.5. It is not always necessary to notify the data subjects or to notify before collection, for example:

18.5.1. where the data subject or a competent person where the data subject is a child has consented to the non-notification;

18.5.2. where non-compliance won't prejudice the legitimate interests of the data subjects;

Example

Where the Responsible party traces a beneficiary.

18.5.3. non-compliance is necessary to avoid prejudice to the maintenance of the law;

Example

Where fraud is suspected.

18.5.4. it is necessary for the conduct of court or tribunal proceedings;

18.5.5. compliance would prejudice a lawful purpose of the collection; or

18.5.6. it is not reasonably practicable in the circumstances of the case.

Guidance notes

- Where notification before collection is not practicable or reasonable, Responsible parties should at least try to notify before using or disclosing the information.
- If the purposes change after collection and such purposes are not compatible with the purposes disclosed, Responsible parties must inform the data subjects of the change in purpose as soon as reasonably possible.

SECURITY SAFEGUARDS

19. SECURITY MEASURES ON INTEGRITY OF PERSONAL INFORMATION

19.1. Responsible parties must secure the integrity and confidentiality of personal information in their possession or under their control by taking appropriate, reasonable technical and organisational measures to prevent:

19.1.1. loss of, damage to or unauthorised destruction of personal information; and

19.1.2. unlawful access to or processing of personal information.[57]

19.2. In order to give effect to the above obligation, Responsible parties must take reasonable measures to:

19.2.1. identify all reasonably foreseeable internal and external risks to personal information;

19.2.2. establish and maintain appropriate safeguards against risks identified;

19.2.3. regularly verify that the safeguards are effectively implemented; and

19.2.4. ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.[58]

19.3. The technical and organisational measures taken must ensure an appropriate level of security.

19.4. Responsible parties must also have due regard to generally accepted information security practices and procedures which may apply to them generally or be required in terms of the Guidelines or other industry or professional rules and regulation.

Guidance notes

- There is no "one size fits all" solution to information security. The security measures that are appropriate for a Responsible party will depend on its circumstances, so Responsible parties should adopt a proportionate risk-based approach to deciding what level of security they need. Appropriate security means that Responsible parties may take into account:
  - the risks involved in processing and the nature of the information to be protected.

[57] Section 19(1).
[58] Section 19(2).

The more sensitive the information, the higher the applied security must be; and

- the state of the art and cost of the implementation measures. The cost of additional measures must be proportionate to the increase in the level of security.

- Responsible parties should:
  - design and organise their security to fit the nature of the personal information they hold and the harm which may result from a security breach;
  - be clear who in the organisation is responsible for ensuring information security;
  - make sure they have the right physical and technical security, backed up by robust policies and procedures and reliable well-trained staff; and
  - be ready to respond to any breach of security swiftly and effectively.
- Responsible parties should, as part of good practice, be in a position to provide evidence of reasonable steps taken to secure personal information.
- Appropriate technical and organisational measures for safeguarding personal information include:
  - agreeing appropriate confidentiality undertakings with employees;
  - preventing unauthorised persons from accessing, altering, disclosing or destroying personal information;
  - ensuring people act within the scope of their authority;
  - checking periodically whether systems require adaptation, for example due to technological developments;
  - ensuring that staff understand the importance of protecting personal information. It is imperative that staff are trained on how to properly deal with personal information, how to properly protect it, and on all applicable policies;
  - encrypting all removable media used for taking personal information offsite; and
  - securing the transmission of personal information.

20. NOTIFICATION OF SECURITY COMPROMISES

20.1. Where there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, the Responsible party must notify the Regulator and the data subjects (unless the identity of the data subjects can't be established) 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.[59]

[59] Section 221.

Guidance note

In determining whether unauthorised access to personal information has been obtained, Responsible parties must assess each case, taking into account POPIA principles, the rights of the data subjects, the needs of their business, the extent of the security compromise, and the extent to which the personal information was secured.

Examples

- Where personal information on laptops and other moveable applications has been secured by means of an acceptable level of encryption and such moveable device is lost or stolen, the personal information on the device will be deemed not to have been accessed or acquired by any unauthorized person.
- Where an email attachment containing personal information of a data subject is sent in error, and that attachment has been secured by means of an acceptable level of encryption, the attachment will be deemed not to have been accessed or acquired by any unauthorized person.

20.2. Notification of security compromises must be in the time and manner prescribed in POPIA.

21. OPERATORS[60]

21.1. Responsible parties will not always process personal information themselves but may have the actual work carried out by an operator. POPIA sets out requirements on the form and content of contracts with operators.

Guidance notes

- It will be necessary for Responsible parties to determine when a third party is acting as an operator.
- Responsible parties must carefully consider their relationships with independent brokers. As long as the broker is processing personal information as part of its business of rendering financial services, the broker should generally not be an operator, but a Responsible party in its own right. However, if the product supplier outsources other services to the broker, the broker may very well be an "operator" for which the Responsible party will be responsible.

Example

Astute is acting as an operator for the Responsible parties when it provides Responsible parties with consolidated client portfolio information.

21.2. Responsible parties do not need the consent of data subjects in order to share personal information with their chosen operator(s). However, other legislation may have

[60] Refer **Chapter 1** for definition of Operator

requirements around consent which should be adhered to.

21.3. Where the processing of personal information is carried out by an operator, the Responsible party must:

21.3.1. ensure that an operator establishes and maintains the security measures which apply to the Responsible party (set out above);

Guidance note

Responsible parties should choose operators providing sufficient undertakings in respect of the technical and organisational security measures governing the processing of personal information to be carried out.

21.3.2. govern the processing by a written contract which requires the operator to establish and maintain the required confidentiality and security measures; and

21.3.3. place a contractual obligation on operators to inform the Responsible party if there was unauthorised access or disclosure of personal information.

21.4. POPIA also imposes a number of independent obligations and restrictions on the operator. The operator must:

21.4.1. process personal information only with the knowledge or authorisation of the Responsible party; and

21.4.2. treat personal information as confidential and not disclose it, unless required by law or in the course of the proper performance of their duties.

DATA SUBJECTS' PARTICIPATION

22. ACCESS TO PERSONAL INFORMATION[61]

22.1. Data subjects have the right to ask a Responsible party to confirm, free of charge, whether or not the Responsible party holds personal information about the data subject.

22.2. Data subjects have the right to ask for 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 who have, or have had access to the information.

22.3. Responsible parties must answer a request for access within a reasonable time (subject to any applicable time periods under PAIA) if they have established proof of identity.

22.4. Responsible parties may charge the prescribed fee for providing the information.

Guidance notes

- Responsible parties should ensure that only data subjects or their clearly chosen representatives have access to their personal information.
- Requests should be answered as soon as reasonably possible, but in any event within

[61] Section 23.

30 days after the request has been received (subject to any applicable time periods under PAIA), unless not reasonably possible, for example where the request is for a large number of records or requires a collation of records from various different divisions or locations.

22.5. When a Responsible party provides the data subjects with the requested information, the Responsible party must inform the data subjects of their right to request correction of the information as specified in POPIA.

22.6. There are limited circumstances under POPIA when data subjects will not be permitted to see information which relates to them. A Responsible party may refuse to disclose information requested where the grounds for refusal of access to records in Chapters 4 of Part 2 and 3 of PAIA apply.

Guidance notes

PAIA Grounds for refusal for private companies (subject to certain exceptions listed in PAIA):

- If its disclosure would involve the unreasonable disclosure of personal information about a third party.
- If the record contains trade secrets or confidential information of a third party.
- If its disclosure would constitute an action for breach of a duty of confidence owed to a third party in terms of an agreement.
- If the disclosure could reasonably be expected to endanger the life or physical safety of an individual or public safety or prejudice the security of a building, property or computer system.
- If the record is subject to legal privilege.
- If the record contains trade secrets or confidential information of the Responsible party.
- If information about research being or to be carried out by or on behalf of a third party, would expose the research or subject matter to its disadvantage.
- If the refusal is in the public interest.

23. CORRECTION OF PERSONAL INFORMATION[62]

23.1. Data subjects are allowed to request Responsible parties to:

23.1.1. correct their personal information if it is inaccurate, irrelevant, excessive[63], out of date, incomplete, misleading or obtained unlawfully; or

23.1.2. destroy a record of personal information which the Responsible party may no longer keep in terms of POPIA.

[62] Section 24.
[63] See section 10 on Minimality.

23.2. Upon receipt of such a request, a Responsible party must:

23.2.1. correct or destroy the information, as the case may be;

23.2.2. notify the data subjects of the actions taken and provide evidence in support thereof or notify the data subjects if the Responsible party refuses to make the correction; and

23.2.3. where the Responsible party is unable to accede to the data subjects' request, and where the data subjects so request, flag the information as having been challenged.

23.3. If a correction of personal information will have an impact on decisions which have been or will be made about the data subjects, the Responsible party must, if reasonably practicable, inform all third parties to whom the information has previously been disclosed of the change.

Guidance notes

- Requests should be answered as soon as reasonably possible, but in any event within 30 days after the request has been received (subject to any applicable time periods under PAIA), unless not reasonably possible.
- A Responsible party does not have to inform third parties if:
    - it is impossible to trace the parties since the Responsible party no longer has the information required for this; and
    - this would involve a disproportionate effort on the Responsible party's part.

Examples

- The applicable industry Life and Claims register
- Representatives of Brokers to the FSCA
- Wrong information of beneficiaries to executor of estate
- Wrong information to bank on policy value
- Wrong information about policyholders to re-insurers

PART THREE - OTHER DATA SUBJECT RIGHTS

DIRECT MARKETING

24. DIRECT MARKETING

Direct Marketing

24.1. Direct marketing means to approach data subjects, either in person, telephone, mail or electronic communication, for the direct or indirect purpose of –

24.1.1. promoting or offering to supply, in the ordinary course of business, any goods or services to the data subjects; or

24.1.2. requesting the data subjects to make a donation of any kind for any reason.

24.2. Data subjects may object, at any time, to the processing of personal information for purposes of direct marketing.

24.3. The question of whether it is permitted to process personal information for direct marketing purposes must be assessed by Responsible parties using the general rules and conditions for lawful processing of personal information set out in POPIA. This means that direct marketing must not be incompatible with the purposes for which the information was acquired.

Example

See 24.4.2.2 below.

Unsolicited electronic communications[64]

24.4. The processing of personal information of data subjects for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail is prohibited, UNLESS the data subjects:

24.4.1. have given their consent to the processing; or

24.4.2. are customers of the Responsible party and if:

24.4.2.1. the data subjects' contact details were obtained in the context of the sale of a Product or Service;

24.4.2.2. the personal information of the data subjects is processed for the purpose of direct marketing of the Responsible party's own similar products or services (in line with 24.3 above); and

24.4.2.3. the data subjects have been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to the use of their electronic details on collection of the information and on each communication for purposes of direct marketing.

24.5. Responsible parties may approach data subjects only once in order to obtain consent for this type of processing.

24.6. Cookies may contain personal information (i.e. cookie identifiers pertaining to the user of a website) and where cookies and/or other tracking software are utilised on websites to track data subject preferences or activities as a means for further direct or indirect on-selling and/or online marketing based on the information received, Responsible parties should ensure that they obtain the consent of the data subjects for the use thereof. Note if personal information is collected by using cookies, the Responsible party must take reasonable steps to make the data subject aware of this and ensure compliance with section 18 of POPIA in this regard.

[64] Section 69.

Example

Utilising cookies on a website to obtain personal information from data subjects with a view to using that information for on-selling and/or further marketing to the data subjects. In such circumstances, consent could be obtained via a simple banner notification such as a header notification or a fixed footer notification, or via a pop-up notice.

AUTOMATED DECISION MAKING

25. DECISIONS BASED ON THE AUTOMATED PROCESSING OF PERSONAL INFORMATION[65]

25.1. Data subjects have the right not to be subject to a decision which results in legal consequences for them or affects them to a substantial degree which is based solely on the basis of automated processing of personal information intended to provide a profile of such person including their performance at work, or their credit worthiness, reliability, location, health, personal preferences or conduct, except if the decision:

25.1.1. has been taken in connection with the conclusion or execution of a contract and:

25.1.1.1. the request of the data subjects in terms of the contract has been met; and

25.1.1.2. appropriate measures have been taken to protect the data subjects' legitimate interests; or

25.1.2. is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of the data subjects.

25.2. The appropriate measures must provide for an opportunity for data subjects to make representations about the decision and provide the data subjects with sufficient information about the underlying logic of the automated processing to make such representations.

Guidance notes

- These rights can be seen as safeguards against the risk that a potentially damaging decision is taken without human intervention.
- These rights only apply to decisions which:
    - involve no human intervention. Many decisions which are regarded as "automated" actually involve human intervention; and
    - which have a significant effect on the data subjects.

[65] Section 71.

PART FOUR - OTHER SUBJECTS

26. PRIOR AUTHORISATION AND UNIQUE IDENTIFIERS[66][67]

Processing subject to prior authorisation[68]

26.1. The Responsible party must obtain prior authorisation from the Regulator if a Responsible party plans to:

26.1.1. 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, unless the processing is authorised by the Regulator in terms of section 37;

26.1.2. process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;

26.1.3. process information for the purposes of credit reporting; or

26.1.4. transfer special personal information or the personal information of children to third parties in foreign countries that do not provide an adequate level of protection.

Examples

- Unique identifiers may include: bank account or other account numbers; policy numbers; SA Identity Numbers or foreign passport numbers; employee numbers; student numbers; telephone or cell phone numbers; or reference numbers.
- Where information is shared with a third-party, for example Astute, prior authorisation may not be required provided that the purpose for sharing the information is clearly stated, compatible with the purposes disclosed, and all the appropriate disclosures are declared upfront.
- Companies within a Group are not considered third parties for which prior authorisation is required under s57(1)(b).
- Credit reporting as defined [69] would not apply to Responsible parties supplying information to third parties (such as credit bureaux) to enable such third parties to in turn compile credit reports.
- Contractual rights to the sharing of information may preclude the need for prior authorisation.

[66] See definition of "*unique identifier*" for purposes of sections 57, 105 and 106 in **Chapter 1**.
[67] See also: Guidance Note on applications for prior authorisation dd 11 March 2021 published by the Information Regulator: https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PriorAuthorisation-20210311.pdf
[68] Section 57
[69] Credit reporting "refers to the processing of personal payment history, lending, and credit worthiness of a data subject by creating a credit report based on that information, and lenders or credit providers use credit reports along with other personal information to determine a data subject's creditworthiness."

26.2. The Responsible party only has to obtain the prior authorisation once and not each and every time that personal information is received or processed, except where the processing departs from that which has been authorised.

Unlawful acts by Responsible parties in connection with account numbers[70]

26.3. For purposes of this section, an account number is any unique identifier that has been assigned to

(a) one data subject only; or

(b) jointly to more than one data subject,

by a financial or other institution which enables the data subjects referred to in paragraph (a), to access their funds or to access credit facilities or which enables data subjects, referred to in paragraph (b), to access joint funds or to access joint credit facilities.

26.4. A Responsible party that contravenes any of the information protection conditions insofar as they relate to the processing of an account number is guilty of an offence **if**:

26.4.1. the contravention is of a serious or persistent nature and is likely to cause substantial damage or distress to the data subjects; and

26.4.2. the Responsible party knew or ought to have known that there was a risk that the contravention would occur, or such contravention would likely cause substantial damage or distress to the data subjects and failed to take reasonable steps to prevent the contravention.

26.5. It is a valid defence to such a charge to contend that the Responsible party has taken all reasonable steps to comply with the information protection conditions.

Unlawful acts by third parties in connection with account numbers[71]

26.6. A person who knowingly or recklessly, without the consent of the Responsible party obtains or discloses an account number of data subjects or procures the disclosure of an account number of data subjects to another person, is guilty of an offence **unless**:

26.6.1. the obtaining, disclosure or procuring of the account number was:

26.6.1.1. necessary for the purpose of the prevention, detection, investigation or proof of an offence; or

26.6.1.2. required or authorised in terms of the law or in terms of a court order;

26.6.2. the Responsible party acted in the reasonable belief that it was legally entitled to obtain or disclose the account number, or as the case may be, to procure the disclosure of the account number to the other person;

26.6.3. the Responsible party acted in the reasonable belief that it would have had the consent of the Responsible party if the Responsible party had known of the obtaining, disclosing or procuring and the circumstances of it or in the particular

[70] Section105.
[71] Section 106.

circumstances the obtaining, disclosing or procuring was in the public interest.

27. TRANSFERS OF PERSONAL INFORMATION OUTSIDE SOUTH AFRICA[72]

27.1. Responsible parties may not transfer personal information about data subjects to a third party in a foreign country unless the third party in question is subject to a law, binding corporate rules[73] or binding agreement which provides an adequate level of protection that -

27.1.1. Effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for lawful processing of personal information relating to data subjects; and

27.1.2. Includes provisions substantially similar to POPIA relating to the further transfer of personal information from the recipient to third parties who are in a foreign country.

27.2. If a third party outside South Africa is not subject to a binding instrument that provides an adequate level of protection in respect of the personal information transferred (as contemplated in clause 27.1), transfer will be possible if:

27.2.1. the data subjects have given their explicit consent for this, or

27.2.2. the transfer is necessary for the performance of the contract between the data subjects and the Responsible party, or for the implementation of pre-contractual measures taken in response to the data subjects' request; or

27.2.3. transfer is necessary for the conclusion or performance of a contract concluded between the Responsible party and a third party in the data subjects' interest, or

27.2.4. transfer is for the benefit of the data subjects, and

27.2.4.1. it is not reasonably practicable to obtain the consent of the data subjects to that transfer; and

27.2.4.2. if it were reasonably practicable to obtain such consent, the data subjects would be likely to give it.

PART FIVE

28. CHECKS ON THE LEVEL OF INFORMATION PROTECTION

28.1. Checks on the level of information protection (e.g. by information protection audits) should be carried out at regular intervals to review the effectiveness and success of the technical and organisational information protection measures implemented. Such audits may be carried out internally by the information officer or other organizational units which have been awarded an audit assignment or, alternatively, by an independent third party approved by the Responsible party.

[72] Section 72
[73] Refer definition of binding corporate rules in Section 72(2)(a)

29. CONTACT DETAILS

Name	Address	Telephone	Fax	eMail
Association for Savings and Investment (ASISA)	Boundary Terraces Bridge House 1 Mariendahl Lane Newlands Cape Town	(021) 673 1620	(021) 673 1630	info@asisa.org.za
Financial Sector Conduct Authority (FSCA)	Riverwalk Office Park, Block B 41 Matroosberg Road Ashlea Gardens, Extension 6 Menlo Park Pretoria	(012) 428 8000	(012) 346 6941	info@fsca.co.za
Information Regulator (South Africa)	JD House 27 Stiemens Street Braamfontein Johannesburg 2001	(012) 406 4818	086 500 3351	inforeg@justice.gov.za
Office of the Ombud for Financial Services Providers (FAIS Ombud)	Eastwood Office Park Baobab House Ground Floor Lynnwood Ridge Pretoria	(012)470 9080	(012) 348 3447	info@faisombud.co.za
Ombudsman for Long-term Insurance	Third Floor, Sunclare Building 21 Dreyer Street Claremont Cape Town	(021) 657 5000	(021) 674 0951	info@ombud.co.za

Responsible Senior Policy Advisor: Taryn Hirsch